Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.2 BC

November 2, 2005

Cisco IOS Release 12.2(15)BC2i

OL-2772-21

These release notes for the Cisco uBR10012 universal broadband router 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)BC2i 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.

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 85 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.

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

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.

Copyright © 2003-2005. Cisco Systems, Inc. All rights reserved.

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 29 and the "Related Documentation" section on page 228.

Cisco IOS Release 12.2(15)BC2i supports the Cisco uBR10012 universal broadband router, which provides a high-capacity, high-throughput cable modem termination system (CMTS), optimized for aggregating traffic at the edge of the cable network. Designed for cable operators and service providers, the platform connects residential subscribers via cable modems, digital set-top boxes, or IP telephony cable modems for high-speed data, broadband entertainment, and IP telephony solutions.

The Cisco uBR10012 router uses the industry-proven Parallel eXpress Forwarding (PXF) technology, derived from the Cisco ESR10000 edge services router, to provide consistent, high-performance throughput, even as software features are added and additional services are deployed.

In addition, it supports a variety of broadband access technologies, including Data-over-Cable Service Interface Specification (DOCSIS), gigabit ethernet, and optical. With support for multiple standards, operators can choose the appropriate services and devices to optimize their capital investment with a single CMTS platform. With access to current and future software enhancements, the Cisco uBR10012 also ensures investment protection as standards and customer needs continue to evolve.

Cable companies and Internet service providers (ISPs) can allocate radio frequency (RF) channel capacity for Internet access or high priority services using a hybrid fiber/coax (HFC) or an all-coax cable plant. Cisco currently provides three router-based DOCSIS CMTS solutions that offer a wider feature set and better manageability than bridge-based systems.

Cisco uBR10012 Universal Broadband Router

The Cisco uBR10012 universal broadband router brings the powerful performance and proven reliability of the industry-leading, DOCSIS-qualified Cisco uBR7200 series universal broadband router product line to the next level of performance, capacity, and throughput. The Cisco uBR10012 platform provides a complete, easy-to-use, integrated router and cable modem termination system (CMTS) package, with feature-rich software and unparalleled customer service and support. With access to current and future software enhancements, the Cisco uBR10012 routers ensure investment protection as standards evolve.

The Cisco uBR10012 router supports up to eight cable interface line cards for connection to subscriber cable modems (CMs) and set-top boxes (STBs). Cisco IOS Release 12.2(15)BC2i supports the Cisco uBR10-MC5X20S-D cable interface line card, Cisco uBR-LCP2-MC16S Spectrum Management Card, Cisco uBR-LCP2-MC16C, Cisco uBR-LCP2-MC16E, and Cisco uBR-LCP2-MC28C cable interface line cards.

Note The LCP versions of the above cable interface line cards have reached end-of-life and are no longer sold, but these cards are still supported by the Cisco uBR10012 router.

For connection to the Internet and other networks, the Cisco uBR10012 router supports up to four network uplink line cards, each of which can support connections as fast as 1Gb/s (Gigabit Ethernet). Cisco IOS Release 12.2(15)BC2i supports OC-12 POS, Gigabit Ethernet connectivity, the Cisco OC-12 DPT line card, and the Cisco OC-48 DPT/POS interface module.

Note For detailed descriptions of the Cisco uBR10012 router chassis and components, see the hardware documents listed in the *"Related Documentation" section on page 228*.

Cisco uBR10012 Router Cable Interface

The cable interface in the Cisco uBR10012 router serves as the RF cable TV interface, supporting downstream and upstream signals. The downstream is output as an IF signal suitable for use with an external upconverter. Your cable plant, combined with your planned and installed subscriber base, service offering, and external network connections, determines what combination of Cisco uBR10012 cable interfaces, network uplink line cards, and other components that you should use.

Cisco IOS Release 12.2(15)BC2i supports the following cable interface line cards, which can be installed in the Cisco uBR10012 chassis in any combination:

- Cisco uBR10-MC5X20S-D cable interface line card, designed for the Cisco uBR10012 router to provide the highest port density, contains five downstream ports and twenty upstream ports, with DOCSIS MAC management and spectrum management capabilities.
- Cisco uBR-LCP2-MC16S Spectrum Management Card with advanced spectrum management features with one downstream and six upstreams.
- Cisco uBR-LCP2-MC16C cable interface line card, based on the existing Cisco uBR-MC16C line card, with one downstream and six upstreams.
- Cisco uBR-LCP2-MC16E cable interface line card, based on the existing Cisco uBR-MC16E line card, with one downstream and six upstreams.
- Cisco uBR-LCP2-MC28C cable interface line card, based on the existing Cisco uBR-MC28C line card, with two downstreams and eight upstreams divided into two domains. This provides the ability to support a large volume of cable modem subscribers using only one chassis.

Note Unless otherwise indicated, all references to the LCP2 versions of the cable interface line cards also apply to the LCP versions of these cards, which have reached end-of-life and are no longer being sold.

All cable interface line cards, except for the Cisco uBR-LCP2-MC16E, support the Data-over-Cable Service Interface Specifications (DOCSIS). DOCSIS 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.

The Cisco uBR-LCP2-MC16E cable interface line card supports the European Data-over-Cable Service Interface Specifications (EuroDOCSIS). EuroDOCSIS 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.

Early Deployment Releases

These release notes describe Cisco IOS Release 12.2(15)BC2i for the Cisco uBR10012 universal broadband router. Release 12.2 XF is an early deployment (ED) release based on Release 12.2 T, which serves as the train's starting point. Early deployment releases contain 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.

Table 2 lists any features supported by the Cisco uBR10012 router in Cisco IOS Release 12.2(15)BC2i. For complete feature information, see the *Cisco uBR10012 Universal Broadband Router Hardware Installation Guide*, the *Field Replaceable Units (FRUs)* documents, and the *Cisco uBR10012 Universal Broadband Router Software Configuration Guide*.

Table 2 Early Deployment (ED) Releases for the Cisco uBR10012 Router

ED Release	Additional Software Features[1] and MIBs[2]	Additional 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)BC2d	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	—
Cisco IOS Release 12.2(15)BC2a	None	None	—

Table 2 Early Deployment (ED) Releases for the Cisco uBR10012 Router (continued)

ED Release	Additional Software Features[1] and MIBs[2]	Additional Hardware Features	Hardware Availability
Cisco IOS Release 12.2(15)BC2	• Advanced TDMA Support • Cable ARP Filter • Command-Line Interface (CLI) Enhancements • Command Enhancements for the Cisco uBR10012 Router • DOCS-IF-MIB Update • Extended Upstream Frequency Ranges • N+1 Support for Load Balancing • PacketCable Enhancements • SNMP Support for Virtual Interfaces • Vendor-Specific Information Field to Authorize Dynamic Service Requests	• Cisco uBR10-MC5X20U	Now
Cisco IOS Release 12.2(15)BC1g	None	None	—
Cisco IOS Release 12.2(15)BC1f	None	None	—
Cisco IOS Release 12.2(15)BC1e	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	—

Table 2 Early Deployment (ED) Releases for the Cisco uBR10012 Router (continued)

ED Release	Additional Software Features[1] and MIBs[2]	Additional Hardware Features	Hardware Availability
Cisco IOS Release 12.2(15)BC1	• Command-Line Interface Enhancements • Dynamic Shared Secret • Load Balancing for the Cisco CMTS • N+1 Operations for the Cisco uBR-MC5X20S Cable Interface Line Card • Nonstop Forwarding (NSF) Awareness—BGP, OSPF, and Integrated IS-IS • PacketCable Support for the Cisco uBR10012 Router • PacketCable Debug Enhancements • Subscriber Traffic Management • Support for Cisco Broadband Troubleshooter Version 3.0 • Virtual Interfaces on the Cisco uBR-MC5X20S Card	None	—
Cisco IOS Release 12.2(11)BC3d	None	None	—
Cisco IOS Release 12.2(11)BC3c	None	None	—
Cisco IOS Release 12.2(11)BC3b	None	None	—
Cisco IOS Release 12.2(11)BC3a	None	None	—
Cisco IOS Release 12.2(11)BC3	• Cisco uBR10012 Route Processor Redundancy Plus (RPR+) and DOCSIS SSO • VLAN Support for the uBR10012 • PBR Support for the uBR10012 • Shared Spectrum Support on the uBR10012 • **clear cable modem** Commands • **debug cable** Commands	• Cisco uBR10-MC5X20S-D cable interface line card • Cisco uBR10012 OC-48 DPT/POS interface module	Now
Cisco IOS Release 12.2(11)BC2a	None	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	—

Table 2 Early Deployment (ED) Releases for the Cisco uBR10012 Router (continued)

ED Release	Additional Software Features[1] and MIBs[2]	Additional Hardware Features	Hardware Availability
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 • N+1 Redundancy Support on Cable Interface Line Cards • Enhancement to the **show hccp brief** Command • Enhancement to the **cable filter group** Command • Advanced Spectrum Management Features: – CNR-based Intelligent Frequency Hopping – CNR-based Dynamic Modulation Change – Dynamic Channel Width Change – Support for Acterna DCMTA v1.1	• Cisco uBR-LCP2-MC16S Spectrum Management Card with Advanced Spectrum Management Features for the Cisco uBR10012 Router	Now
Cisco IOS Release 12.2(8)BC1	• EXEC Commands in Configuration Mode • Secure Shell (SSH)	• Cisco uBR-LCP2 Cable Interface Line Card • Support for 128 MB Flash Cards	Now
Cisco IOS Release 12.2(4)BC1b	• DOCSIS 1.1 N+1 Redundancy • SNMP Cable Modem Remote Query	• None	—
Cisco IOS Release 12.2(4)BC1	• Support for the **cable power** command	• Cisco uBR10-SRP-OC12SML DPT WAN Card	Now
Cisco IOS Release 12.2(4)XF1	• N+1 Redundancy for the Cisco CMTS	• Cisco uBR-RFSW RF switch	Now

Table 2 Early Deployment (ED) Releases for the Cisco uBR10012 Router (continued)

ED Release	Additional Software Features[1] and MIBs[2]	Additional Hardware Features	Hardware Availability
Cisco IOS Release 12.2(4)XF	• Route Processor Redundancy (RPR) support • Support for the **cable monitor** command	• Cisco uBR-LCP-MC16C Cable Interface Line Card • Cisco uBR-LCP-MC16E Cable Interface Line Card • PRE1 Performance Routing Engine • DC PEM with power supply monitoring connector	Now
Cisco IOS Release 12.2(2)XF1	None	None	
Cisco IOS Release 12.2(2)XF	None	None	
Cisco IOS Release 12.2(1)XF1	• DOCSIS 1.0 and 1.1 Support • DOCSIS Baseline Privacy Interface (BPI) encryption and authentication	None	

Table 2 Early Deployment (ED) Releases for the Cisco uBR10012 Router (continued)

ED Release	Additional Software Features[1] and MIBs[2]	Additional Hardware Features	Hardware Availability
Cisco IOS Release 12.2(1)XF	• Address Verification • Basic Wiretap Support • Guided Frequency Hopping • Broadband Internet Access • Cable Interface Bundling • Cable Interface Setup Facility • Cable Modem Transmission Burst Size • Cisco IOS Quality of Service Features • Configurable Registration Timeout • Customer Premises Equipment Limitation and Override • DOCSIS 1.0 Support • Downstream Channel ID Configuration • Downstream Frequency Override • Dynamic or Mobile Host Support • Dynamic Modulation Profiles • Dynamic Ranging • Dynamic Upstream Modulation • Flap List Support • Host-to-Host Communication (Proxy Address Resolution Protocol) • Integrated DHCP and Time-of-Day Servers • IP Broadcast and Multicast Echo • Modulation Profile Configuration • MPLS-VPN Network Support • Packet Interception • Simple Network Management Protocol Management Information Base • Simple Network Management Protocol v3 • Spectrum Management • Statistical Counters	• Cisco uBR10012 Router • PRE Performance Routing Engine • Cisco uBR-LCP-MC28C Cable Interface Line Card • Timing, Communication, and Control Plus Card Description • Gigabit Ethernet Line Card • OC-12 POS Line Card • DC Power Entry Modules • 2400-Watt AC-Input Power Shelf • Fan Assembly Module • LCD Display Panel	Now

1. Only major features are listed.
2. MIB = Management Information Base

System Requirements

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

Memory Recommendations

Table 3 displays the memory recommendations of the Cisco IOS feature sets for the Cisco uBR10012 universal broadband router for Cisco IOS Release 12.2(15)BC2i. Cisco uBR10012 universal broadband routers are available with a 48-MB or 120-MB Type II PCMCIA Flash memory card or 128 MB Flash Disk card.

Table 3 Memory Recommendations for the Cisco uBR10012 Routers, Cisco IOS Release 12.2(15)BC2i Feature Sets

Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
DOCSIS BPI IP Plus	ubr10k-k8p6-mz[1]	40 MB Flash	128 MB DRAM	RAM

1. The Cisco IOS 12.2(11)BC3 image cannot be loaded from a 128 MB Flask Disk. This image is not available in the Cisco IOS 12.2(11)BC2a rebuild release.

Note In Cisco IOS Release 12.2(11)BC3 only, the ubr10k-k8p6-mz software image could not be loaded from a 128 MB Flash Disk card. See caveat CSCea65301 in Bug Toolkit for more information. This caveat was fixed, and this limitation removed, in Cisco ISO 12.2(11)BC3a and later Release 12.2 BC releases.

Supported Hardware

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 29. Cisco IOS Release 12.2(15)BC2i supports the following hardware on Cisco uBR10012 routers:

Table 4 Cisco uBR10012 Universal Broadband Router Overview

Cable Interface Line cards	Up to eight of the following cable interface line cards can be housed in a chassis in any combination: • Cisco uBR10-MC5X20S-D • Cisco uBR-LCP2-MC16S spectrum management card • Cisco uBR-LCP2-MC16C • Cisco uBR-LCP2-MC16E • Cisco uBR-LCP2-MC28C • Cisco uBR-LCP2-MC28C-B
Network Uplink Line Cards	Up to four line cards with any combination of the following WAN choices: • Cisco uBR10012 OC-48 DPT/POS interface module • uBR10-1GE Gigabit Ethernet (GigE) uplink line card • uBR10-1OC12/P-SMI OC-12 POS uplink line card • uBR10-SRP-OC12SML Dynamic Packet Transport (DPT) WAN card **Note** Cisco IOS Release 12.2(15)BC2i does not support the CISCO-SRP-MIB.my MIB for the Cisco uBR10-SRP-OC12SML DPT WAN card.
Timing, Communication and Control Plus (TCC+) card	The TCC+ card can connect to an external reference Stratum 3 clock source that is traceable to a Stratum 1 source. Two such sources can be connected for redundancy. The TCC+ card also monitors the cable line cards and power supply use, as well as control the LCD display screen on the chassis. Two cards can be installed for redundancy.
Performance Routing Engine (PRE or PRE1)	One PRE or PRE1 module performs layer 2 and layer 3 packet processing, as well as routing and system management functions. Two PRE or PRE1 modules can be installed for redundancy. **Note** The PRE1 module is functionally identical to the PRE module except that it adds support for the Error Checking and Correction (ECC) feature, which can automatically correct single-bit memory errors.

Table 4 Cisco uBR10012 Universal Broadband Router Overview (continued)

DC-input Power Entry Module (PEM)	Two DC PEMs provide power to the chassis. The use of two PEMs provide power balancing and redundancy, as well as the ability to hot-swap a single power supply when needed.
Fan assembly module	The fan assembly module contains four fans that are capable of cooling the chassis even with the failure of a single fan. The fan assembly is dual-speed, providing additional cooling when the chassis temperature exceeds the nominal operating range.

Note The Cisco uBR10012 router is compatible with Cisco Broadband Troubleshooter 2.0 and Cisco Cable Manager 2.0.

Determining Your Software Release

To determine the version of Cisco IOS software running on the Cisco uBR10012 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 (uBR10k-k8p6-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 5 lists the features and feature sets supported by the Cisco uBR10012 routers 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.

Note This table 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. For a list of the 12.1 T-train features in this platform, refer to Feature Navigator. For more information about Feature Navigator, see the "Cisco Feature Navigator" section on page 230.

The asterisk (*) in Table 5 indicates that the feature set and its image are not available in the Cisco IOS 12.2(11)BC2a rebuild release. The feature set and image are available in Cisco IOS Release 12.2(15)BC2i.

Table 5 Feature List by Feature Sets for Cisco uBR10012 Universal Broadband Routers

Feature	Feature Set DOCSIS IP Plus with BPI *
IP Routing	
802.1 Q VLAN Support	Yes
DOCSIS 1.0 and 1.1 Support	Yes
DHCP[1] Server	Yes
DRP[2] Server Agent	Yes
IP Enhanced IGRP[3] Route Authentication	Yes
IP Fragmentation Support	Yes
IP Multicast Echo Support	Yes
Multicast Routing (MFIB) Support	Yes
Nonstop Forwarding (NSF) Awareness—BGP, OSPF, and Integrated IS-IS	Yes
Policy-Based Routing Support	Yes
Unicast Routing (FIB) Support	Yes
Management	
BPI[4] and BPI+ MIB	Yes
Cable Intercept (CALEA) Support	Yes
Cable Intercept (CALEA) Support for PacketCable Operations	No
Cable Interface Dual Hardware Queue Support	Yes
Cable Interface Flow Control Support	Yes
Cisco Broadband Troubleshooter Version 3.0 Support	Yes
Cisco Call History MIB Command Line Interface	Yes
Cisco IOS Internationalization	Yes
DOCSIS Ethernet MIB Objects Support (RFC 2665)	Yes
DOCSIS OSSI[5] Objects Support (RFC 2233)	Yes
DOCSIS 1.1 N+1 Redundancy Support on Cable Interface Line Cards	Yes
Dynamic Ranging Support	Yes
Entity MIB, Phase 1	Yes
Gigabit Ethernet Line Card Support	Yes
Interface Bundling	Yes
Interface Command Enhancements	Yes
Internal Modem Configuration File Editor	Yes

Table 5 Feature List by Feature Sets for Cisco uBR10012 Universal Broadband Routers (continued)

Feature	Feature Set DOCSIS IP Plus with BPI *
LinkUp/Down Traps Support (RFC 2233)	Yes
Load Balancing for the Cisco CMTS	Yes
MIB Enhancements	Yes
N+1 Operations for the Cisco uBR-MC5X20S Cable Interface Line Card	Yes
OC-12 POS Line Card	Yes
PacketCable Support for the Cisco uBR10012 Router	Yes
RF Interface MIB	Yes
Route Processor Redundancy Plus (RPR+) and DSSO[6]	Yes
SNMP Cable Modem Remote Query	Yes
SNMPv2C[7] and SNMPv3[8]	Yes
Subscriber MIB Packet Filtering	Yes
Virtual Interfaces on the Cisco uBR-MC5X20S Card	Yes
Multimedia	
Bidirectional PIM[9]	Yes
Stub IP Multicast Routing	Yes
Quality of Service	
252 Operator Configurable QoS Service Profiles for DOCSIS 1.0	Yes
Admission Control for Load Balancing	Yes
Admission Control (Including Weighting Functions per QoS Profile)	Yes
DHCP/PPoE Packet Divert Support	Yes
DOCSIS 1.0 Configuration File Editor (IOS CLI-based)	Yes
DOCSIS 1.0+[10] QoS Enhancements	Yes
Downstream DOCSIS 1.1 Classification Support	Yes
Downstream DOCSIS 1.1 Queuing Support	Yes
Downstream QoS Handling	Yes
Downstream Traffic Shaping	Yes
Dynamic Map-Advance	Yes
Dynamic Upstream Modulation	Yes
Guaranteed Upstream Minimum Throughput per Modem for DOCSIS 1.0	Yes
Improved Upstream QoS	Yes
JIB Upstream Header Support	Yes
JIB Downstream Header Support	Yes

Table 5 Feature List by Feature Sets for Cisco uBR10012 Universal Broadband Routers (continued)

Feature	Feature Set DOCSIS IP Plus with BPI *
Modular QoS CLI Support (for non-cable interfaces)	Yes
Class-Based Weighted Fair Queuing (CB-WFQ)	Yes
Low Latency Queuing (LLC)	Yes
Shaping	Yes
Multiple SID Support for DOCSIS 1.0+	Yes
Multiple SID Support for DOCSIS 1.1	Yes
Multiple SID Support (static only)	Yes
QoS Configuration	Yes
QoS Policy Propagation via Border Gateway Protocol (QPPB)	Yes
QoS Profile Enforcement	Yes
QoS Profile Management via SNMP, IOS CLI, or Dynamic	Yes
RTP[11] Header Compression	Yes
Shared Spectrum Support	Yes
Subscriber Traffic Management	Yes
Time of Day (ToD) Server	Yes
ToS Bit Restamping and ToS-based QoS for DOCSIS 1.0	Yes
ToS Overwrite Support	Yes
Upstream Address Verification	Yes
Upstream Traffic Shaping	Yes
Security	
Automated Double Authentication	Yes
BPI and BPI+ Encryption	Yes
Cable source-verify	Yes
Cable source-verify DHCP, Including lease-query	Yes
Cisco IOS Firewall Enhancements	Yes
Dynamic Mobile Hosts	Yes
Dynamic Shared Secret	Yes
HTTP[12] Security	Yes
IP Security Access List Support	Yes
Named Method Lists for AAA[13] Authorization & Accounting	Yes
Per-User Configuration	Yes
Secure Shell (SSH)	Yes
SNMP Access Lists, Including Logging Features	Yes
TACACS+	Yes

Table 5 Feature List by Feature Sets for Cisco uBR10012 Universal Broadband Routers (continued)

Feature	Feature Set DOCSIS IP Plus with BPI *
TFTP-enforce	Yes
VPN/MPLS	
MPLS Disposition Support	
MPLS Imposition on Cable Subinterfaces Support	Yes
MPLS VPN Support for Subinterfaces and Interface Bundles	Yes
WAN Optimization	
PAD[14] Subaddressing	Yes

1. DHCP = Dynamic Host Configuration Protocol
2. DRP = Director Response Protocol
3. IGRP = Interior Gateway Routing Protocol
4. BPI = Baseline Privacy Interface
5. OSSI = Operations Support System Interface
6. DSSO = DOCSIS Stateful Switchover
7. SNMPv2 = Simple Network Management Protocol version 2
8. SNMPv3 = Simple Network Management Protocol version 3
9. PIM = Protocol Independent Multicast
10. 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.
11. RTP = Real-Time Transport Protocol
12. HTTP = Hypertext Transfer Protocol
13. AAA =authentication, authorization, and accounting
14. PAD = packet assembler/disassembler

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(15)BC2i that apply to the Cisco uBR10012 universal broadband router.

Limitations 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 6 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.)

Access Lists on the Cisco uBR10012 Router

The Parallel eXpress Forwarding (PXF) processors on the Cisco uBR10012 router provide the increased performance of Turbo Access Control Lists (Turbo ACL) by default by automatically compiling all access lists when access lists are configured.

You do not need to use the **access-list compiled** command to enable the Turbo ACL feature. You can display these access lists by using the **show access-lists** command without the **compiled** option.

Note The Cisco uBR10012 router does not compile simple access lists that have a small number of rules, because it is more efficient to process these lists in the standard manner than to compile them. The State column in the **show access-lists compiled** command identifies these access lists as "Non TA Operational."

For complete information about access lists, see the "Traffic Filtering and Firewall" volume in the *Cisco IOS Release 12.1 Security Configuration Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/index.htm

Acterna DCMTA v1.1 Tool

The Acterna DCMTA v1.1 tool is no longer available from Acterna, starting with Cisco IOS Release 12.2(15)BC1.

The Cisco Broadband Troubleshooter 3.0 (CBT) replaces the DCMTA tool. 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

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
```

BPI+ Multicast is Not Supported on Bundled Subinterfaces

BPI-encrypted multicasts are not supported on the Cisco uBR10012 router on cable subinterfaces that are also configured as part of a bundle. BPI-encrypted multicasts are supported on bundled cable interfaces or on cable subinterfaces, but not on bundled cable subinterfaces.

Cable Device, Host, and Modem Commands Not Supported

The Cisco uBR10012 universal broadband router does not support the following commands:

- **cable device access-group**
- **cable host access-group**
- **cable modem access-group**

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.

Changes to the cable source-verify Command

In Cisco IOS Release 12.2(15)BC1 and later releases, the **cable source-verify dhcp** command extends IP address verification to CPE devices that had been online using a valid IP address but then were reconfigured by the user with an unused static IP address. With Cisco IOS Release 12.2(15)BC1 and later, CPE devices are not allowed online when they are using static IP addresses that have not been allocated by the DHCP server. If you are using the **cable source-verify** command with the **dhcp** option, the CPE device must use an IP address that has been assigned by the DHCP server.

Caution 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).

Changes to the cable tftp-enforce Command

In Cisco IOS Release 12.2(15)BC1 and later releases, when the **cable tftp-enforce** command is configured on the cable interface, the Cisco uBR10012 router can occasionally allow a cable modem to temporarily come online before the system has received confirmation that the cable modem has downloaded the proper DOCSIS configuration file. This situation can occur when the cable interface line card receives a registration request (REG-REQ) message from a cable modem before the PRE1 module has notified the line card whether the modem did download the proper file from the TFTP server.

In previous Cisco IOS releases, these cable modems were not allowed to come online (or marked as TFTP violators) even if they had successfully downloaded the appropriate DOCSIS configuration file. In Cisco IOS Release 12.2(15)BC1 and later releases, however, the Cisco uBR10012 router allows these cable modems to temporarily come online until the PRE1 module has finished determining the modem's TFTP status. If the system determines that the modem did not download the appropriate DOCSIS configuration file, it is then taken offline (or marked as a TFTP violator).

Note In the above situation, cable modems that do not download a DOCSIS configuration file are marked as "offline" instead of "reject(c)" by the **show cable modem** command. The console still displays the %UBR10000-4-REGISTRATION_BEFORE_TFTP error message, however, to allow you to identify these cable modems as TFTP violators.

Configuring the CMTS Cable Interface When Configuring a CM for Routing Mode

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 uBR10012 router with the **cable dhcp-giaddr policy** command. Otherwise, the cable interface could flap and the CM could go offline unpredictably.

Configuring the Routing Protocol Causes a Reset of the Cable Modems

Be aware that when configuring a routing protocol, 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 routing global configuration commands, such as **router rip**, on a cable interface only when a minimum of subscribers would be affected.

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.

Deleting Internal Access Lists Can Cause System Malfunction

The Cisco uBR10012 router uses internal access lists for various functions. These internal access lists do not appear in the running configuration but are displayed in the **show access-list** output for debugging purposes. The internal access lists are prefixed with 'CMTS_PKT_FILTER_GROUP'.

If these access lists are removed using the Global Configuration CLI, the router can malfunction, including resulting in a system failure.

The following is an example of how an ACL is deleted in Global Configuration mode:

```
conf t
no ip access-list extended CMTS_PKT_FILTER_GROUP_255
end
```

This issue is documented in CSCin54155 in Cisco IOS Release 12.2(15)BC1. The workaround is to not delete or disable these internal access-lists.

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

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.

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

The Cisco uBR10012 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.

FastEthernet Interface Automatically Negotiates

The FastEthernet interface on the PRE1 module (interface F0/0/0) ignores the link speed and duplex settings but instead always automatically negotiates the correct speed and duplex settings with the device at the other end of the connection.

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 configuration 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 appears 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-modem 0**.
- 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).

Minimum Revision for the Cisco uBR-LCP Line Card Processor

The Cisco uBR-LCP line processor card must be at revision 4.4 or greater and be using the boothelper image from Cisco IOS Release 12.2(2)XF1 or later to support the Cisco uBR-MC16C and Cisco uBR-MC16E cable interface line cards.

PRE PXF Resets Unexpectedly

The Performance Routing Engine (PRE) Parallel eXpress Forwarding (PXF) processors can reset unexpectedly while generating the following ICMP response packets — ICMP Echo Reply, ICMP network unreachable, and ICMP TTL expired when any of the following features are configured:

- input Packet Intercept
- input ACL with logging
- input ACL with more than 255 entries
- input Packet Filter Group with more than 255 packet filters
- input QoS config on the backhaul interfaces with more than 255 entries

Use one of the following possible workarounds:

- Do not configure the above mentioned features, or
- Take the following steps to minimize ICMP response packet generation by PXF processors:
  - Add a default route to a valid next-hop to avoid generation of ICMP network unreachable packets by the PXF.
  - Drop ICMP echo requests to the primary address of the CMTS interfaces to avoid generation of ICMP echo response by the PXF.

Note that pings to the secondary addresses are not handled by the PXF.

Note There is no user configurable command to avoid generation of ICMP TTL expired.

This issue is documented in caveat CSCea75288 in Cisco IOS Release 12.2(11)BC3a and resolved in Cisco IOS Release 12.2(11)BC3b.

PRE Module Not Supported

The Cisco uBR10012 router supports only the PRE1 module in Cisco IOS Release 12.2(8)BC1, and later releases including Cisco IOS Release 12.2(11)BC3. If you attempt to boot the Cisco uBR10012 router with one of these software releases and a PRE module, the router will print the following error message and fall through to the ROM monitor:

```
%%Error: PRE not supported with this image rommon>
```

To correct this error, replace the PRE modules in the router with PRE1 modules. To continue using the original PRE modules, you must reload the router with Cisco IOS Release 12.2(4)BC1 or an earlier 12.2 BC release.

Redundant PRE Modules Are Not Supported Before Release 12.2(4)XF

Cisco IOS Release 12.2(4)XF introduced support for the Route Processor Redundancy (RPR) feature for the Performance Routing Engine (PRE) cards. This allows two PRE modules to be installed in a Cisco uBR10012 chassis for redundant operation.

Earlier releases of software for the Cisco uBR10012 router do not support RPR. In these earlier releases, two PRE modules can be installed in a Cisco uBR10012 chassis, but Cisco does not guarantee that upon a failure of the primary PRE module, the redundant PRE module can automatically bring up all DOCSIS cable interface line cards.

For more information about the RPR feature, see the *Route Processor Redundancy (RPR) on the Cisco uBR10012 Universal Broadband Router* feature module, available on Cisco.com and the Customer Documentation CD-ROM.

Removing IGMP Static Groups on Cable Interfaces

When you use the **no ip igmp static-group** command to remove an IGMP static group on a master cable subinterface, the mroute entries still exist for all of the slave interfaces.

To complete the removal, you must also use the following commands to remove the IGMP configuration on the slave cable interfaces:

```
clear ip mroute <multicast address>
clear ip igmp group <master or subinterface>
```

For more information on the commands, refer to the *Cisco IOS Command Reference, Release 12.2 T* at the following URL:

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

Reformatting Flash Cards Required in Release 12.2(11)BC3a and Later

Flash Disk cards that were formatted using Cisco IOS software releases 12.2(4)BC1 through 12.2(8)BC2 should be reformatted using Cisco IOS Release 12.2(11)BC3a or later. Flash Disk cards formatted with these earlier software releases could have intermittent timing problems that

could prevent files from being read on the disks and thus prevent a PRE1 module from booting using the software on the disk.

Show Interface Counters are Separate for Master and Slave Interfaces

The Cisco uBR10012 router uses a distributed architecture that does not include the slave interface input packet counters when you use the **show interface** command to display information for a master cable interface. This is different than normal behavior for most Cisco interfaces, where the input packet counters on the master interface include the input packet counts for all associated slave interfaces. On the Cisco uBR10012 router, you must use the **show interface** command on both the master and slave cable interfaces to get a total count of the input packets.

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.

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.

Unsupported Counter for Policy Maps

The "Packets marked" counter that is displayed by the **show policy-map interface** command is not supported on the Cisco uBR10012 router and always shows 0. However, the first "packets" counter for each Class-map is also the "Packets marked" value, so use the "packets" counter for both values.

For example, the following output shows that the "Packets marked" counter is 0, but the "packets" value is 1000, which means the "Packets marked" counter is also 1000 packets.

```
Router# show policy-map interface GigabitEthernet 4/0/0
 GigabitEthernet4/0/0
  Service-policy input:set

   Class-map:matchany (match-any)
   1000 packets, 1024000 bytes
   5 minute offered rate 0 bps, drop rate 0 bps
   Match:any
   QoS Set
    qos-group 3
     Packets marked 0
```

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.

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

Using the show cable modem Command After an HCCP Switchover

If you are using HCCP 1+1 or N+1 Redundancy, the new primary processor after a switchover automatically creates a new database of the online cable modems. This means that the **show cable modem** *ip-address* and **show cable modem** *ip-address* **cnr** commands might not show a particular cable modem until the CMTS receives IP traffic from that cable modem.

You can force IP traffic by using the **ping** *ip-address* command, and then the **show cable modem** *ip-address* and **show cable modem** *ip-address* **cnr** commands will show the cable modem. You can also display any particular cable modem by using the **show cable modem | include** *ip-address* command.

Use of the FastEthernet Port on the PRE Module

The FastEthernet interface on the PRE module is intended for network management access and should not be used for WAN connectivity purposes. For WAN connections, use the appropriate network uplink cards, which take full advantage of the system's high-performance PXF processing subsystem.

Web Cache Communication Protocol Is Not Supported

The Cisco uBR10012 router does not support the Web Cache Communication Protocol (WCCP) feature set in Cisco IOS Release 12.2(15)BC2i.

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**.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco uBR10012 router for Cisco IOS Release 12.2(15)BC2i. These sections also show the features inherited since Cisco IOS Release 12.2(2)XF1.

For more information about these features, refer to the documents listed in the "Related Documentation" section on page 228.

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)BC2d

There are no new hardware features in Cisco IOS Release 12.2(15)BC2d.

New Software Features in Release 12.2(15)BC2d

There are no new software features in Cisco IOS Release 12.2(15)BC2d.

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.

New Hardware Features in Release 12.2(15)BC2

The following hardware feature is new in Cisco IOS Release 12.2(15)BC1.

Cisco uBR10-MC5X20U

The Cisco uBR10-MC5X20U cable interface line card is one of the new Broadband Processing Engine (BPE) series of cable interfaces that are available for the Cisco uBR10012 universal broadband router. The BPE cards provide increased performance and advanced Radio Frequency (RF) management, as well as innovative, integrated tools for sophisticated content, traffic and network management.

The Cisco uBR10-MC5X20U contains five downstream ports and twenty upstream ports. Each downstream port includes an onboard integrated upconverter that generates an RF signal suitable for connection to a combiner and transmission on the coaxial cable network, without the need for any external upconverters.

In Cisco IOS Release 12.2(15)BC2 and later releases, the downstream ports support 64-QAM and 256-QAM, and the upstream ports support QPSK, 8-QAM, 16-QAM, 32-QAM, and 64-QAM modulation, depending on the upstream's mode of operation. The upstream ports are initially configured to form five DOCSIS MAC domains, with each downstream port having four upstream ports. However, in Cisco IOS Release 12.2(15)BC2 and later releases, you can use the Virtual Interface feature to configure upstream ports as desired.

Depending on the configuration, the Cisco uBR10-MC5X20U line card supports either DOCSIS or Euro-DOCSIS operation:

- DOCSIS cable networks are based on the ITU J.83 Annex B physical layer standard and Data-over-Cable Service Interface Specifications (DOCSIS, Annex B) specification, which use 6 MHz National Television Systems Committee (NTSC) channel plans. In this mode, the downstream uses a 6 MHz channel width in the 85 to 860 MHz frequency range, and the upstream supports multiple channel widths in the 5 to 42 MHz frequency range.
- EuroDOCSIS cable networks are based on the ITU J.112 Annex A physical layer standard and European DOCSIS (EuroDOCSIS, Annex A) specification, which use 8 MHz Phase Alternating Line (PAL) and Systeme Electronique Couleur Avec Memoire (SECAM) channel plans. In this mode, 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.

When operating in either the DOCSIS or EuroDOCSIS mode of operation, the Cisco uBR10-MC5X20U card supports the following types of networks:

- TDMA-only mode, which supports only DOCSIS 1.0 and DOCSIS 1.1 cable modems.
- A-TDMA-only mode, which supports DOCSIS 2.0 cable modems.
- Mixed TDMA/A-TDMA mode, which supports both DOCSIS 1.0/DOCSIS 1.1 and DOCSIS 2.0 cable modems on the same upstream.

Note The Cisco uBR10-MC5X20U card also supports the extended frequency ranges that are used in Japanese Annex B networks: 70 to 860 MHz (downstream) and 5 to 55 Mhz (upstream).

For information on installing the Cisco uBR-MC5X20U card, see the *Cisco uBR10-MC5X20S/U Cable Interface Line Card*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/frus/ubrmc520.htm

For information on configuring the Cisco uBR-MC5X20U card, see the *Configuring the Cisco uBR10-MC5X20U-D Cable Interface Line Card*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/mc5x20u.htm

Note The **load-interval** interface configuration command is not supported on the Cisco uBR-MC5X20S/U cable interface line cards, even though the CLI accepts the command for these interfaces.

New Software Features in Release 12.2(15)BC2

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

Advanced TDMA Support

Cisco IOS Release 12.2(15)BC2 supports the A-TDMA Service feature, which provides support for DOCSIS 2.0 Advanced Time Division Multiple Access (A-TDMA) upstream modulation profiles on the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20S/U Broadband Processing Engine (BPE) cable interface line cards. This feature supplements the existing support for DOCSIS 1.0 and DOCSIS 1.1 Time Division Multiple Access (TDMA) modulation profiles.

For more information on the A-TDMA service feature, see the *Configuring A-TDMA Modulation Profiles* document, at the following URL:

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

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

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-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 time zone for the file's date and time. The time zone 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

Command Enhancements for the Cisco uBR10012 Router

Cisco IOS Release 12.2(15)BC2 added or enhanced the following commands on the Cisco uBR10012 router:

- **cable per-cpe-acl**—Defines an access list (ACL) to be applied on a Cisco uBR10012 router to customer premises equipment (CPE) devices that are currently unknown, providing a way to control the network access of unknown CPE devices. The Cisco uBR10012 router applies the specified ACL to any CPE device that is not in its host tables, or that does not have another ACL applied to its IP or MAC addresses.
- **debug cr10k-rp ha-error** and **debug cr10k-rp ha-recovery**—New commands to aid in troubleshooting N+1 HCCP redundancy operation.
- All **show hardware pxf** commands have been renamed as **show pxf**.
- **switchover pxf restart**—Specifies the maximum number of times that a PXF processor can crash during a specified time period before the router switches over to the redundant PRE-1 module. If the PXF processors crash this number of times, the router assumes a hardware problem and initiates a switchover to the redundant PRE-1 module.

For more information on these commands, see the *Commands for the Cisco uBR10012 Router* document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/bbub10k.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).

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

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.

SNMP Support for Virtual Interfaces

The Virtual Interfaces feature allows a physical upstream connector to be associated as a logical upstream interface for use with any downstream. Previously, an upstream was hard-coded for use with a particular downstream, but the Virtual Interfaces feature allows each physical upstream connector on the card to be mapped as a logical upstream interface for use with any of the other downstreams.

The Virtual Interfaces feature was initially supported in Cisco IOS Release 12.2(15)BC1 for the Cisco uBR-MC5X20S cable interface line card. Cisco IOS Release 12.2(15)BC2 added support for Virtual Interfaces on the Cisco uBR-MC5X20U cable interface line card, and also introduced SNMP support for Virtual Interfaces.

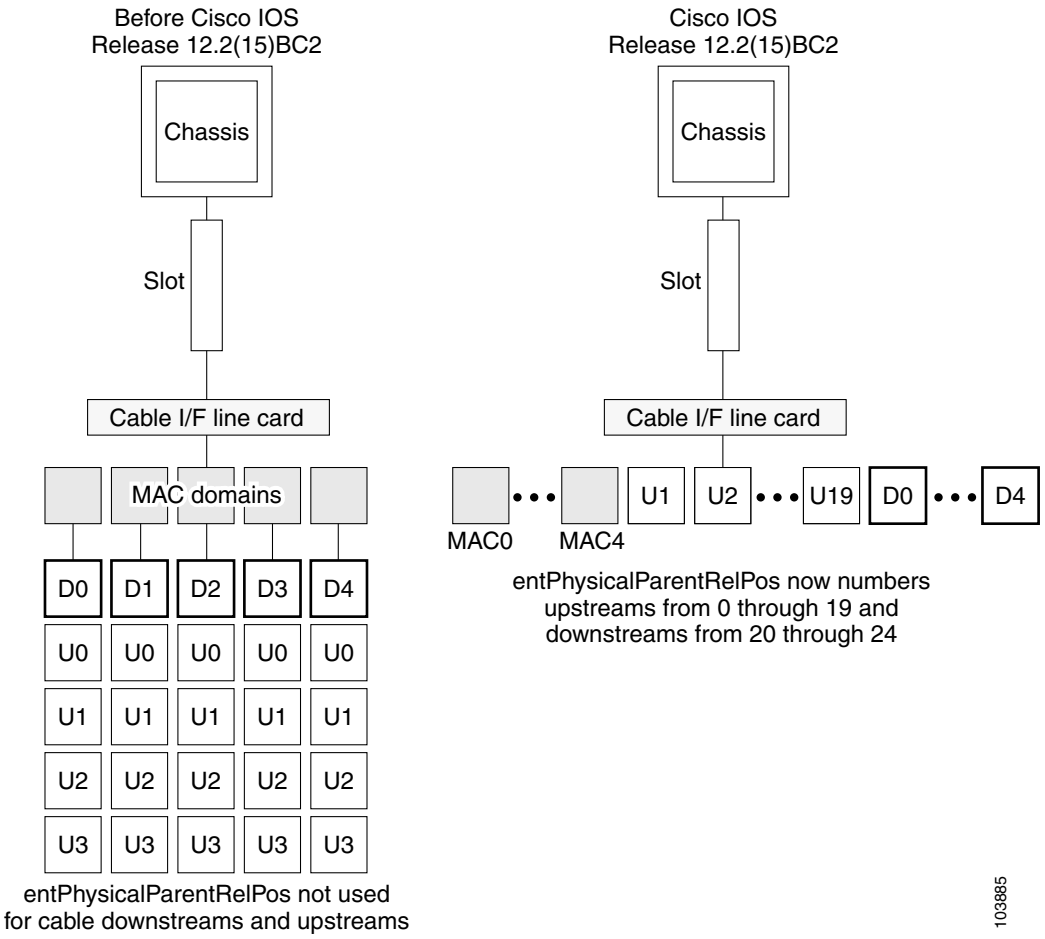
Changes to ENTITY-MIB

To enable SNMP support for Virtual Interfaces, Cisco IOS Release 12.2(15)BC2 changed how the entPhysicalTable in the ENTITY-MIB displays the information for cable interface line cards. Previously, the cable interface line card was the parent to one or more MAC domains, and each MAC domain then was the parent to one downstream and one or more upstreams.

Because an upstream can now be associated with any MAC domain and downstream in Cisco IOS Release 12.2(15)BC2, the ENTITY-MIB no longer associates upstreams and downstreams with specific MAC domains, but instead shows all of them as being children of the line card. The entityPhysicalParentRelPos also now numbers the upstreams in sequential order, followed by the downstreams, so that on the Cisco uBR-MC5X20S cards, the upstreams are numbered from 0 to 19, and the downstreams from 20 to 24.

Figure 1 shows the difference in how the entPhysicalTable in the ENTITY-MIB organized a Cisco uBR-MC5X20S cable interface line card in previous releases and in Cisco IOS Release 12.2(15)BC2. For consistency, all cable interface line cards use this approach, even if they do not support the Virtual Interfaces feature.

Figure 1 ENTITY-MIB Changes for Virtual Interface Support on Cable Interface Line Cards



Operation of the ENTITY-MIB with Virtual Interfaces

The following are the key points in how the ENTITY-MIB shows the physical relationship of objects when the Virtual Interfaces feature is configured:

- The entPhysicalTable shows information only about the physical card and its connectors. This table's configuration is fixed when the router boots or when a new card is installed in the chassis, and this configuration is not updated to show any logical mappings.

  The entPhysicalTable index numbers for the card and its ports never change unless the card is physically removed and another type of card is installed in its slot. For example, if the entPhysicalName.50 object returns a value of "Cable6/1-US0" after the router boots, it always returns this value, no matter how the card and its upstream ports are configured.

  For example, the Cisco uBR-MC5X20S and Cisco uBR-MC5X20U cards contain 20 upstreams, which the entPhysicalTable numbers from 0 to 19, regardless of how the upstreams are mapped using Virtual Interfaces. Similarly, the entPhysicalParentRelPos objects number the 20 upstreams as children 0 through 19, and the 5 downstreams as children 20 through 24. This numbering never changes, regardless of the Virtual Interfaces configuration.

- The mapping between the physical upstream connectors and the logical upstream interfaces is shown in the entityAliasMappingTable. Each entry in this table contains the ifDescr index (as defined in the ifTable in the IF-MIB) that maps to the physical connector that is being used for that interface. The Virtual Interfaces feature automatically updates the entityAliasMappingTable to show the mapping between the physical upstream connectors and the logical interfaces, whenever the **cable upstream connector** is used.

For example, when a Cisco uBR-MC5X20S card is installed in slot 8/1 in a Cisco uBR10012 router, the ENTITY-MIB would typically list the upstreams similar to the following (the exact index numbers would depend on the number and type of other cards that are installed in the chassis):

```
!
entPhysicalDescr.81 = LBT4522 PHY
entPhysicalDescr.82 = LBT4522 PHY
...
entPhysicalDescr.99 = LBT4522 PHY
entPhysicalDescr.100 = LBT4522 PHY
!
entPhysicalVendorType.81 = cevPortRfUs
entPhysicalVendorType.82 = cevPortRfUs
...
entPhysicalVendorType.99 = cevPortRfUs
entPhysicalVendorType.100 = cevPortRfUs
!
entPhysicalName.81 = Cable8/1-US0
entPhysicalName.82 = Cable8/1-US1
...
entPhysicalName.99 = Cable8/1-US18
entPhysicalName.100 = Cable8/1-US19
```


Note The index numbers shown in entPhysicalTable never change during normal operation of the router. For example, using the above sample output, index 81 in the entPhysicalTable always points to the first upstream on the card in slot 8/1 (Cable8/1-US0). This index numbering is guaranteed to remain the same until you either reboot the router or until you change the router's physical configuration by adding or removing hardware components.

The default configuration for the Cisco uBR-MC5X20S automatically maps each physical connector to its default logical interface (physical connector 0 maps to C8/1/0U0, connector 1 maps to C8/1/0U1, and so on, until physical connector 19 maps to C8/1/4U3). Using the above example, the entAliasMappingIdentifierTable defaults to a configuration similar to the following:

```
entAliasMappingIdentifier.81.0 = ifIndex.28 (ifDescr.28 = Cable8/1/0-upstream0)
entAliasMappingIdentifier.82.0 = ifIndex.29 (ifDescr.29 = Cable8/1/0-upstream1)
entAliasMappingIdentifier.83.0 = ifIndex.30 (ifDescr.30 = Cable8/1/0-upstream2)
entAliasMappingIdentifier.84.0 = ifIndex.31 (ifDescr.31 = Cable8/1/0-upstream3)
entAliasMappingIdentifier.85.0 = ifIndex.33 (ifDescr.33 = Cable8/1/1-upstream0)
entAliasMappingIdentifier.86.0 = ifIndex.34 (ifDescr.34 = Cable8/1/1-upstream1)
entAliasMappingIdentifier.87.0 = ifIndex.35 (ifDescr.35 = Cable8/1/1-upstream2)
entAliasMappingIdentifier.88.0 = ifIndex.36 (ifDescr.36 = Cable8/1/1-upstream3)
entAliasMappingIdentifier.89.0 = ifIndex.38 (ifDescr.38 = Cable8/1/2-upstream0)
entAliasMappingIdentifier.90.0 = ifIndex.39 (ifDescr.39 = Cable8/1/2-upstream1)
entAliasMappingIdentifier.91.0 = ifIndex.40 (ifDescr.40 = Cable8/1/2-upstream2)
entAliasMappingIdentifier.92.0 = ifIndex.41 (ifDescr.41 = Cable8/1/2-upstream3)
entAliasMappingIdentifier.93.0 = ifIndex.43 (ifDescr.43 = Cable8/1/3-upstream0)
entAliasMappingIdentifier.94.0 = ifIndex.44 (ifDescr.44 = Cable8/1/3-upstream1)
entAliasMappingIdentifier.95.0 = ifIndex.45 (ifDescr.45 = Cable8/1/3-upstream2)
entAliasMappingIdentifier.96.0 = ifIndex.46 (ifDescr.46 = Cable8/1/3-upstream3)
entAliasMappingIdentifier.97.0 = ifIndex.48 (ifDescr.48 = Cable8/1/4-upstream0)
entAliasMappingIdentifier.98.0 = ifIndex.49 (ifDescr.49 = Cable8/1/4-upstream1)
entAliasMappingIdentifier.99.0 = ifIndex.50 (ifDescr.50 = Cable8/1/4-upstream2)
entAliasMappingIdentifier.100.0 = ifIndex.51 (ifDescr.51 = Cable8/1/4-upstream3)
```

The entAliasMappingIdentifierTable mapping, however, can change whenever the **cable upstream connector** command is used to enable the Virtual Interfaces feature. For example, upstream 2 on C8/1/4 is normally mapped to physical upstream connector 18 (entPhysicalTable index 99), but it can be mapped to physical upstream connector 0 (entPhysicalTable index 81) with the following commands:

```
Router(config)# interface cable 8/1/4
Router(config-if)# cable upstream 2 connector 0
Router(config-if)#
```

In the default configuration, the ENTITY-MIB shows the following for these two upstreams:

```
entPhysicalName.81 = Cable8/1-US0
entPhysicalName.99 = Cable8/1-US18
entAliasMappingIdentifier.81 = ifIndex.28 (ifDescr.28 = Cable8/1/0-upstream0)
entAliasMappingIdentifier.99 = ifIndex.50 (ifDescr.50 = Cable8/1/4-upstream2)
```

After the **cable upstream connector** command is used, the ENTITY-MIB is updated as follows. (Note that only the entAliasMappingIdentifier objects have changed.)

```
entPhysicalName.81 = Cable8/1-US0
entPhysicalName.99 = Cable8/1-US18
entAliasMappingIdentifier.81 = ifIndex.50 (ifDescr.50 = Cable8/1/4-upstream2)
entAliasMappingIdentifier.99 =
```

Note The above example shows that physical connector upstream 0 is now mapped to the logical interface upstream 2 on Cable 8/1/4, and that physical connector upstream 18 is no longer in use. Its entAliasMappingIdentifier will return NULL until the **cable upstream connector** command maps another logical upstream to this particular physical connector.

DOCSIS Configuration File Changes for Type-Length-Value (TLV)

Note A Type-Length-Value (TLV) is a tuple within a DOCSIS or PacketCable configuration file.

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. This is illustrated below with the Type-Length-Value (TLV) of 43:

- 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 enables 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)
```

Additional information about the TLV value on the Cisco CMTS is available in these documents:

- *Cisco Broadband Access Center for Cable Administrator's Guide Release 2.7*

  http://www.cisco.com/en/US/partner/products/sw/netmgtsw/ps529/products_administration_guide_book09186a008037ca63.html
- *Cisco CMTS Configuration FAQ*, TAC Document 12180

  http://www.cisco.com/en/US/tech/tk86/tk804/technologies_q_and_a_item09186a00800a4ae5.shtml
- *DHCP and the DOCSIS Configuration File for Cable Modems* , TAC Document 10961

  http://www.cisco.com/en/US/tech/tk86/tk168/technologies_tech_note09186a0080180f11.shtml

DSX Values in the TLV Field

Cisco IOS Release 12.2(15)BC2 supports a new TLV value for DSX/DSA. Dynamic Service Exchange is a DOCSIS 1.1 QoS signaling mechanism providing Dynamic Service Add, Change and Delete functions (reference PacketCable specification PKT-TR-MM-ARCH-V01-030627).

- The new TLV value of 12 supports DSX/DSA enable and disable functions
- By default, all DSX requests are allowed.

Additional information about the TLV value on the Cisco CMTS is available in these documents:

- *Cisco Broadband Access Center for Cable Administrator's Guide Release 2.7*

  http://www.cisco.com/en/US/partner/products/sw/netmgtsw/ps529/products_administration_guide_book09186a008037ca63.html
- *Cisco CMTS Configuration FAQ*, TAC Document 12180

  http://www.cisco.com/en/US/tech/tk86/tk804/technologies_q_and_a_item09186a00800a4ae5.shtml
- *DHCP and the DOCSIS Configuration File for Cable Modems* , TAC Document 10961

  http://www.cisco.com/en/US/tech/tk86/tk168/technologies_tech_note09186a0080180f11.shtml

IGMP Blanket Forwarding in the TLV Field for Routing Information Protocol (RIP)

Cisco IOS Release 12.2(15)BC2 introduces a new TLV value for IGMP forwarding, in support of the Routing Information Protocol (RIP):

- The new TLV value of 135 enables the cable modem to support blanket IGMP forwarding requests, per RIP.
- By default, blanket IGMP forwarding is disabled.

Cisco IOS Release 12.3(13a)BC introduces support for Internet Group Management Protocol (IGMPv3) Source Specific Multicast (SSM). This enhancement provides support for virtual interface bundling on the Cisco CMTS. IGMP is used by IPv4 systems to report their IP multicast group memberships to any neighboring multicast routers. Additional information about IGMP is available in the following documents:

- *Multicast Support for IGMPv3 SSM and Virtual Interface Bundling*

  http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008022eba7.html#wp1042051

Additional information about Routing Information Protocol is available in the following document:

- *Configuring Routing Information Protocol*

  http://www.cisco.com/en/US/partner/products/sw/netmgtsw/ps529/products_administration_guide_chapter09186a008034777a.html#wp1213805

Additional information about the TLV value on the Cisco CMTS is available in these documents:

- *Cisco Broadband Access Center for Cable Administrator's Guide Release 2.7*

  http://www.cisco.com/en/US/partner/products/sw/netmgtsw/ps529/products_administration_guide_book09186a008037ca63.html
- *Cisco CMTS Configuration FAQ*, TAC Document 12180

  http://www.cisco.com/en/US/tech/tk86/tk804/technologies_q_and_a_item09186a00800a4ae5.shtml
- *DHCP and the DOCSIS Configuration File for Cable Modems* , TAC Document 10961

  http://www.cisco.com/en/US/tech/tk86/tk168/technologies_tech_note09186a0080180f11.shtml

show cable modem verbose

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 shows "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)BC1e

There are no new hardware features in Cisco IOS Release 12.2(15)BC1e.

New Software Features in Release 12.2(15)BC1e

There are no new software features in Cisco IOS Release 12.2(15)BC1e.

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.

Load Balancing for the Cisco CMTS

The Load Balancing on the Cisco CMTS feature allows service providers to optimally use both downstream and upstream bandwidth, enabling the deployment of new, high-speed services such as voice and video services. This feature also can help reduce network congestion due to the uneven distribution of cable modems across the cable network and due to different usage patterns of individual customers.

By default, the Cisco CMTS platforms use a form of load balancing that attempts to equally distribute the cable modems to different upstreams when the cable modems register. You can refine this form of load balancing by imposing a limit on the number of cable modems that can register on any particular upstream, using the **cable upstream admission-control** command.

However, this default form of load balancing affects the cable modems only when they initially register with the Cisco CMTS. It does not dynamically rebalance the cable modems at later times, such as when they might change upstream channels in response to RF noise problems, or when bandwidth conditions change rapidly because of real-time traffic such as Voice over IP (VoIP) and video services. It also does not affect how the cable modems are distributed among downstream channels.

For more information about the Load Balancing feature, see the Configuring Load Balancing on the Cisco CMTS document, at the following URL:

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

N+1 Operations for the Cisco uBR-MC5X20S Cable Interface Line Card

Cisco IOS Release 12.2(15)BC1 supports N+1 HCCP redundancy when using the Cisco uBR-MC5X20S cable interface line card on the Cisco uBR10012 router. For information on configuring and using N+1 redundancy, see the N+1 Redundancy for the Cisco CMTS chapter in the Cisco CMTS Feature Guide, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufgnpls1.htm

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

PacketCable Support for the Cisco uBR10012 Router

Cisco IOS Release 12.2(15)BC1 supports PacketCable operations for the Cisco uBR10012 router, in addition to the existing support for the Cisco uBR7246VXR router. For information on configuring and using PacketCable, see the PacketCable for the Cisco CMTS chapter in the Cisco CMTS Feature Guide, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_pkcb.htm

PacketCable Debug Enhancements

The following **debug** commands have been added or enhanced to support PacketCable operations:

- **debug packetcable ipc**
- **debug packetcable cops**
- **debug packetcable gate events process**
- **debug packetcable subscriber**

In addition, most of the other debug packetcable commands have been modified so that they display output only when the appropriate **debug packetcable subscriber** command has been given. For a complete description of these commands and the changes, see the Cisco CMTS Debugging 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/bbcmtsde.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

Virtual Interfaces on the Cisco uBR-MC5X20S Card

The Virtual Interfaces feature provides additional flexibility and efficiency in the allocation and usage of the upstreams on the Cisco uBR-MC5X20S card for the Cisco uBR10012 universal broadband router. By default, four upstreams are assigned to each downstream, but this feature allows providers to associate any combination of upstreams (up to 8) to each downstream.

The onboard processors on the Cisco uBR-MC5X20S card provides the processing power necessary to allow configurable MAC domains, so that the upstreams are no longer fixed by their physical location, but can be assigned to any of the five downstreams on the card, depending on the particular requirements of each MAC domain.

For more information about the Virtual Interfaces feature, see the Configuring Virtual Interfaces on the the Cisco uBR-MC5X20S Card document, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122bc/122bc_15/mc5x2vif.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)BC3a

There are no new hardware features in Cisco IOS Release 12.2(11)BC3a.

No New Software Features in Release 12.2(11)BC3a

There are no new software features in Cisco IOS Release 12.2(11)BC3a.

New Hardware Features in Release 12.2(11)BC3

Cisco IOS Release 12.2(11)BC3 supports the following new hardware feature for the Cisco uBR10012 router.

Support for the Cisco uBR10-MC5X20S Cable Interface Line Card

The Cisco uBR10-MC5X20S cable interface line card, is designed for the Cisco uBR10012 router to provide the highest port density available in Cisco cable interface line cards. The Cisco uBR10-MC5X20S cable interface line card is a 20 by 16 inch card, that transmits and receives RF signals between the subscriber and the headend over a hybrid fiber/coax (HFC) system.

The Cisco uBR10-MC5X20S cable interface line card supports downstream and upstream traffic over a Data-Over-Cable Service Interface Specification (DOCSIS)-based cable modem network. The card supports all DOCSIS 1.1-specified Annex B radio frequency (RF) data rates, channel widths, and modulation schemes and has DOCSIS MAC management and spectrum management capabilities.

The Cisco uBR10-MC5X20S cable interface line card supports 6-MHz National Television Systems Committee (NTSC) channel operation, using standard (STD), Harmonic Related Carrier (HRC), or Incremental Related Carrier (IRC) frequency plans conforming to EIA-S542. The card supports downstream channels in the 88 to 860 MHz range, and upstream channels in the 5 to 42 MHz range.

The Cisco uBR10-MC5X20S cable interface line card contains five downstream ports and twenty upstream ports. The downstream ports support 64-QAM and 256-QAM, and the upstream ports support QPSK and 16-QAM modulation.

Each downstream port includes an onboard integrated upconverter that generates an RF signal suitable for connection to a combiner and transmission on the coaxial cable network, without the need for any external upconverters. This can save both the money and rack space required by an external upconverter, as well as reduce the complexity of the equipment at the headend site.

Upstream data from the subscriber, comes through the upstream ports (US0-US19) on the Cisco uBR10-MC5X20 cable interface line card. The line card processes and configures the data and sends it across the backplane to the WAN card and out to the Internet.

Downstream data to the subscriber, comes from the Internet through the WAN card, and across the backplane to the Cisco uBR10-MC5X20 cable interface line card. The Cisco uBR10-MC5X20S card processes and configures the data and sends it out through the appropriate downstream port (DS0 - DS4) to be combined with the rest of the downstream signals in the headend. Each downstream port includes an inboard integrated upconverter.

The Cisco uBR10-MC5X20S-D cable interface line card is available with space-saving dense (D) connectors.

Table 7 shows the supported DOCSIS modulation schemes.

Table 7 Supported DOCSIS Modulation Schemes

Cable Interface Line Card	Downstream Modulation	Upstream Modulation
Cisco uBR10-MC5X20S-D	QAM–64, QAM-256	QPSK, QAM-16

Restrictions

- Cisco IOS Release 12.2(11)BC3 and the Cisco uBR10-MC5X20S cable interface line card require the use of the Cisco PRE1 module in the Cisco uBR10012 universal broadband router. If you are using redundant processors, both processors must be Cisco PRE1 modules.

- The following software features are not supported for the Cisco uBR10-MC5X20S cable interface line card with Cisco IOS Release 12.2(11)BC3:
  - Cable Monitor
  - HCCP 1+1 and N+1 redundant configurations (this feature is supported in Cisco IOS Release 12.2(15)BC1 and later releases)
  - Point-to-Point Protocol over Ethernet (PPPoE)
- The Cisco uBR10-MC5X20S cable interface line card includes onboard spectrum analyzer hardware. However, card support for advanced spectrum management features on the Cisco uBR10-MC5X20S cable interface line card will commence with future Cisco IOS releases. Future advanced spectrum management support will include all features currently available with the Cisco uBR-LCP2-MC16S cable interface line card.
- The configuration of the downstream and upstream ports is fixed into five domains. (This restriction is removed when using the Virtual Interfaces feature in Cisco IOS Release 12.2(15)BC1 and later releases.)
- The **load-interval** interface configuration command is not supported on the Cisco uBR-MC5X20S/U cable interface line cards, even though the CLI accepts the command for these interfaces.

Note For information on additional limitations and restrictions for the Cisco uBR10-MC5X20S cable interface line card, see Cisco uBR-MC5X20S Cable Interface Line Card, page 78 in the Limitations and Restrictions section of this release note.

Note For information on installing and cabling the Cisco uBR10-MC5X20S-D cable interface line card, refer to the FRU document, *Cisco uBR10-MC5X20S Cable Interface Line Card*. For information on configuring the Cisco uBR10-MC5X20S-D cable interface line card, refer to the New Features document, *Configuring the Cisco uBR10-MC5X20S Cable Interface Line Card*.

OC-48 DPT Support for the uBR10012

The Cisco uBR10012 OC-48 Dynamic Packet Transport (DPT)/POS interface module is a dual mode module, providing interface support for Packet over SONET (POS) or Spatial Reuse Protocol (SRP).

The Cisco uBR10012 OC-48 DPT/POS interface module supports SONET Section Data Communications Channel (SDCC) in either POS or SRP modes.

- POS technology is ideally suited for Internet and/or IP networks, because it provides superior bandwidth utilization efficiency over other transport methods. POS can support a single connection or redundant connections to provide a robust, high-speed, high-throughput transport for IP traffic.
- SRP is the media-independent Media Access Control (MAC)-layer protocol that enables DPT functionality in ring configurations. The SRP MAC protocol provides the base functionality for addressing, packet stripping, bandwidth control, and control message propagation on the packet ring.

The Cisco uBR10012 OC-48 DPT/POS interface module has a pair of OC-48c, fiber-optic standard connector (SC) duplex ports that provide an SC connection for either the single-mode short-reach or single-mode long-reach version.

Note When using the **show interface pos** or **show interface srp** commands to display information about an interface, be aware that the byte counters used for these commands are 32-bit counters, which have a maximum size of approximately 4.3 billion. The result is the byte counters could wrap back to 0 if the Cisco uBR10012 OC-48 DPT/SRP interface module is passing large amounts of traffic.

For additional information on the Cisco uBR10012 OC-48 DPT/POS interface module, refer to the following documentation:

- *Configuring the Cisco uBR10012 OC-48 DPT/POS Interface Module at:* http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/ub10ksw/ub1048p1.htm
- Quick Start Guide for installing the Cisco OC-48 DPT/POS interface module at the following Cisco uBR10012 Quick Start Guide Index: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/qsg/index.htm
- Field Replaceable Unit (FRU) document for the Cisco OC-48 DPT/POS interface module at the following Cisco uBR10012 FRU Index: http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/frus/index.htm

New Software Features in Release 12.2(11)BC3

Cisco IOS Release 12.2(11)BC3 supports the following new software features for the Cisco uBR10012 router.

Cisco uBR10012 Route Processor Redundancy Plus and DOCSIS SSO

Cisco IOS Release 12.2(11)BC3 introduces support for Route Processor Redundancy Plus (RPR+) and DOCSIS Stateful Switchover (DSSO) on the Cisco uBR10012 universal broadband router.

RPR+ in combination with DSSO enhances the high-availability and redundancy offered by the earlier Route Processor Redundancy (RPR) feature on the Cisco uBR10012 router.

In standard RPR, the standby route processor (RP) suspended its initialization midway through the startup process. To complete the initialization during a switchover, all line cards were reset and the switch fabric was reinitialized.

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

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

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

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

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

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

Note Encrypted multicast broadcast is not supported during a PRE1 switchover.

Note For information on RPR+ restrictions, see Route Processor Redundancy Plus (RPR+), page 79 in the Limitations and Restrictions section of this release note.

For more information on the RPR+ feature, refer to the feature module *Route Processor Redundancy Plus on the Cisco uBR10012 Universal Broadband Router* at the following Cisco uBR10012 Router Software Features index:

http://www.cisco.com/univercd/cc/td/doc/product/cable/ubr10k/ubr10012/ub10ksw/index.htm

VLAN support for the Cisco uBR10012

Cisco IOS IEEE 802.1Q provides support for IEEE 802.1Q encapsulation for Virtual LANs (VLANs). VLANs can be implemented with Cisco IOS platforms in environments where the IEEE 802.1Q encapsulation standard is required. With the introduction of the Cisco IOS IEEE 802.1Q Support feature, Cisco IOS supported 802.1Q VLAN encapsulation, in addition to the currently supported ISL and IEEE 802.10 SDE encapsulations.

Release 12.2(15)BC2i adds 802.1Q VLAN support for the Cisco uBR10012 universal broadband router. Service providers can use 802.1Q VLANs on gigabit Ethernet interfaces to provide isolation between different content providers' traffic. 802.1Q VLANs may be mapped to MPLS VPN, maintaining traffic separation across an MPLS infrastructure.

For more information, refer to the *IEEE 802.1.Q Configuration* guide at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/mar_3200/mar_conf/m511m80.htm

Refer also to the *Cisco IOS IEEE 802.1Q Support* guide for command reference information at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/8021q.htm#xtocid1367322

PBR support for the Cisco uBR10012

Policy-Based Routing (PBR) provides a tool for expressing and implementing the forwarding or routing of data packets, on the basis of the policies that are defined by network administrators. PBR allows policy override on routing protocol decisions by selectively applying policies based on access list and/or packet size.

Network administrators can also use PBR to selectively change the IP ToS, IP precedence, and IP QoS Group fields for matching incoming packets on an interface.

The Cisco uBR10012 universal broadband router supports a maximum of 255 PBR policies and 32 route maps within each policy. The following subset of policy-based routing commands is supported in this release of Cisco IOS software:

- **ip policy route-map map-tag**
- **route-map map-tag** [**permit** | **deny**] [*sequence-number*]
- **match ip address** {*ACL-number* | *ACL-name*} [*ACL-number* | *ACL-name* ...]
- **match length min max**
- **set** [**default**] **interface type number** [*type number* ...]
- **set ip** [**default**] next-hop ip-address [ip-address ...]
- set ip precedence value

- set ip qos-group value
- set ip tos value
- show route-map [map-tag]

For more information on PBR, refer to the "Configuring Policy-Based Routing" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt1/qcfpbr.htm

Shared Spectrum Support on the uBR10012

Cisco IOS Release 12.2(11)BC3 adds support for the **cable spectrum-group shared** command for the Cisco uBR-LCP2-MC16S cable interface line card. The **cable spectrum-group shared** command in global configuration mode allows the upstream ports in a spectrum group to share the same upstream frequencies. The default upstream port frequency is the same for all ports in the spectrum group.

Because this command forces upstream ports to use the same spectrum, do not use this command for overlapping carriers. This command also does not enable any sort of load balancing on the shared upstreams.

For syntax and important usage information, 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

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)BC2a

There are no new hardware features in Cisco IOS Release 12.2(11)BC2a.

No New Software Features in Release 12.2(11)BC2a

There are no new software features in Cisco IOS Release 12.2(11)BC2a.

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

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.

New Hardware Features in Release 12.2(8)BC2

Cisco IOS Release 12.2(8)BC2 supports the following new hardware feature for the Cisco uBR10012 router.

Cisco uBR-LCP2-MC16S Spectrum Management Card with Advanced Spectrum Management Features for the Cisco uBR10012 Router

The Cisco uBR-LCP2-MC16S cable interface line card has a DOCSIS-based cable interface that supports one downstream and six upstreams. It incorporates a daughter board with hardware-based spectrum management features that provide the following features:

- Integrates a DOCSIS cable interface line card with an onboard spectrum analyzer that continuously analyzes the upstream spectrum quality in the DOCSIS frequency range of 5 to 42 MHz
- Includes hardware-assisted frequency hopping, providing for more intelligent and faster frequency selection than software-only solutions
- Reduces the response time to ingress noise that could cause modems to drop offline
- Eliminates guided frequency hopping by initiating frequency hops to known clean channels
- Improves frequency agility to help eliminate dropped packets and thereby maintain full upstream data rates
- Supports frequency agility in dense-mode combining environments across a shared spectrum
- Restricts frequency hopping to a set of discrete frequencies or to a range of frequencies, as desired
- Allows frequency hop conditions to be customized for specific plant environments and requirements
- Optionally schedules frequency hops to take advantage of known usage patterns or plant conditions
- Optionally dynamically reduces channel width to allow cable modems to remain online, even in noisy upstream conditions
- The Cisco uBR-LCP2-MC16S line card can be installed in existing deployments of the Cisco uBR10012 router.

- As is the case with the other cable interface line cards, the Cisco uBR-LCP2-MC16S line card supports Online Insertion and Removal (OIR), allowing for hotswappable upgrades and maintenance

The Advanced Spectrum Management Features for the Cisco uBR-LCP2-MC16S cable interface line card, available in Cisco IOS Release 12.2(8)BC2, are a software-only upgrade that provides the following additional features:

- Supports proactive channel management to avoid the impacts of ingress and keep subscribers online and connected.
- Offers flexible configuration choices, allowing users to determine the priority of the actions to be taken when ingress noise on the upstream exceeds the allowable thresholds. The configurable actions are frequency hopping, switching the modulation profile, and reducing the channel width.
- Performs CNR calculations using DSP algorithms in real-time on a per-interface and per-modem basis.
- Intelligently determines when to modify the frequency, channel width, or modulation scheme based on CNR calculations in the active channel. Previously, frequency and channel width changes occurred when the number of missed station maintenance polls exceeded a user-defined threshold.
- Enhances the Dynamic Upstream Modulation feature for the Cisco uBR-LCP2-MC16S line card. This feature supports dynamic modulation using two upstream profiles. The primary profile (typically using 16 QAM modulation) remains in effect at low noise conditions, but if upstream conditions worsen, the cable modems switch to the secondary profile (typically using QPSK modulation) to avoid going offline. When the noise conditions improve, the modems are moved back to the primary profile.

  When using a Cisco uBR-LCP2-MC16S line card on a Cisco uBR7200 series router running Cisco IOS Release 12.2(8)BC2, the spectrum management hardware uses the real-time CNR readings from the DSPs on the MC16S daughter card instead of the signal-to-noise ratio (SNR) values from the Broadcom 3137 chip to determine the signal quality of the upstream channel. The CNR value is a more accurate description of noise conditions on the upstream.
- Provides an SNMP interface to so that a network management workstation or other graphical tool can obtain spectrum information for either a particular cable modem or for an entire upstream. The frequency resolution can be as fine as 12 KHz.

  Note The CISCO-CABLE-SPECTRUM MIB has been enhanced to provide this support.

- Supports Cisco Broadband Troubleshooter 3.0 (CBT), starting with Cisco IOS Release 12.2(15)BC1. CBT replaces the DCMTA tool from Acterna. CBT 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

- In Cisco IOS Release 12.2(8)BC2, supported management tools include the DOCSIS Cable Modem Test Analyzer (DCMTA) from Acterna. The DCMTA software provides spectrum analyzer capability for an individual upstream port or an individual cable modem. Spectrum data is extracted from the Cisco uBR-MC16S cable interface line card using SNMP, allowing for live troubleshooting of an upstream port or individual cable modem. The DCMTA software supports simultaneous client access to a single or multiple CMTS, upstreams, or cable modems.

  In Cisco IOS Release 12.2(15)BC1 and later, the Acterna DCMTA tool is no longer available from Acterna.

  Note To contact Acterna about the DCMTA software, call 1-800-Acterna or visit http://www.acterna.com.

New Software Features in Release 12.2(8)BC2

Cisco IOS Release 12.2(8)BC2 supports the following new software features for the Cisco uBR10012 router.

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 3/0. 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 3/0
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: %UBR7200-4-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 3/0
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
Cable3/0/U1 1     online(pt)  2734    0.50  5   0   10.1.1.38       00ff.fffa.0a35
Cable3/0/U0 2     online(pt)  2729    0.25  5   0   10.1.1.50       00ff.ff07.382f
Cable3/0/U0 3     init(i)     2732    0.25  2   0   10.1.1.48       00ff.ff03.307d
Cable3/0/U1 4     online(pt)  2737    0.75  5   0   10.1.1.34       00ff.ff59.4477
Cable3/0/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 c3/0 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 Cable3/0/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 %UBR7200-4-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 Cable3/0/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: %UBR7200-4-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 3/0
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
Cable3/0/U1 1     online(pt)  2734    0.50  5   0   10.1.1.38       00ff.fffa.0a35
Cable3/0/U0 2     online(pt)  2729    0.25  5   0   10.1.1.50       00ff.ff07.382f
Cable3/0/U0 3     init(i)     2732    0.25  2   0   10.1.1.48       00ff.ff03.307d
Cable3/0/U1 4     online(pt)  2737    0.75  5   0   10.1.1.34       00ff.ff59.4477
Cable3/0/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 Cable3/0/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: %UBR7200-4-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

N+1 Redundancy Support on Cable Interface Line Cards

In Cisco IOS Release 12.2(8)BC2, the Cisco uBR10012 now supports N+1 Redundancy on the Cisco uBR-MC16S, Cisco uBR-MC16C, and Cisco uBR-MC16E cable interface line cards on DOCSIS 1.1 networks.

Cisco IOS Release 12.2(4)BC1b introduced DOCSIS 1.1 N+1 Redundancy for the Cisco uBR10012. This feature extended the previous HCCP 1+1 cable interface redundancy feature, where one cable interface is designated the working interface, and a second cable interface is the protect interface. The protect interface comes online only when the working interface fails. The N+1 Redundancy feature allowed a single cable interface to act as the protect interface for up to 7 cable interfaces in the Cisco uBR10012 router, thereby significantly reducing the cost of providing redundant operation. The cable interface connections are made through the Cisco uBR-RFSW RF Switch.

In Cisco IOS Release 12.2(8)BC2, the Cisco uBR-MC16S card can be used as the protect cable interface or working cable interface, with either another Cisco uBR-MC16S card or a Cisco uBR-MC16C card. Table 8 shows how a switchover in each of these configurations affects the intelligent spectrum management features of the Cisco uBR-MC16S card.

Table 8 Switchover Operation for a Cisco uBR-MC16C/Cisco uBR-MC16S Configuration

Working Cable Interface	Protect Cable Interface	Operation After Switchover
Cisco uBR-MC16C	Cisco uBR-MC16S	The protect card (Cisco uBR-MC16S) uses the same upstream frequency as the working card, but after the system stabilizes, the protect card begins using the intelligent spectrum management features of the Cisco uBR-MC16S card, as configured on the protect CMTS.
Cisco uBR-MC16S	Cisco uBR-MC16C	The protect card (Cisco uBR-MC16C) uses the same upstream frequency as the working card. If the upstream becomes unstable, the Cisco uBR-MC16C performs only guided frequency hopping.
Cisco uBR-MC16S	Cisco uBR-MC16S	The protect card initially uses the same upstream frequency as the working card, but after the system stabilizes, the protect card continues using the intelligent spectrum management features of the Cisco uBR-MC16S card.

Note Encrypted multicast broadcast is not supported across a line card switchover.

Note For complete information about the N+1 Redundancy feature, see the "N+1 Redundancy for the Cisco CMTS" chapter in the *Cisco CMTS Feature Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufgnpls1.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

Router#
```

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

Support for LCP2 Cable Interface Line Cards

Cisco IOS Release 12.2(8)BC1 adds support for the LCP2, the Enhanced Line Card Processor. The LCP2 cable interface line card is compatible with the previous LCP cable interface line card and can be used in place of the Line Card Processor (LCP) for any currently supported cable interface line card.

Table 9 LCP and LCP2 Cable Interface Line Cards Comparison

Cable Interface Line Card	Processor Speed	Memory Interface Speed
LCP	263 MHz	75 MHz
LCP2	400 MHz	100 MHz

The order numbers for the LCP2 and cable interface line card combinations are:

- UBR10-LCP2, UBR10-LCP2= Line Card Processor 2 card.
- UBR10-LCP2-MC16E, UBR10-LCP2-MC16E= Cisco uBR-MC16E and LCP2 card combination.
- UBR10-LCP2-MC16C, UBR10-LCP2-MC16C= Cisco uBR-MC16C and LCP2 card combination.
- UBR10-LCP2-MC28C, UBR10-LCP2-MC28C= Cisco uBR-MC28C and LCP2 card combination.
- UBR10-LCP2-MC28-B, UBR10-LCP2-MC28-B= Cisco uBR-MC28C-BNC and LCP2 card combination.

Support for 128 MB Flash Cards

Cisco IOS Release 12.2(8)BC1 adds support for the 128 MB Flash Disk card (product order number ESR-PRE-MEM-FD128=).

New Software Features in Release 12.2(8)BC1

The following new software features are supported by the Cisco uBR10012 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 uBR10012 router, 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 the Cisco uBR10012 router, use the following command in global configuration mode:

```
uBR10k(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 uBR10012 router, use the following command in Privileged EXEC mode:

```
uBR10k# show ip ssh

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

To verify whether the Cisco uBR10012 router has an SSH connection, use the following command in Privileged EXEC mode:

```
uBR10k# 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

Cisco IOS Release 12.2(4)BC1b includes support for the following new software features.

DOCSIS 1.1 N+1 Redundancy

The DOCSIS 1.1 N+1 Redundancy for the Cisco CMTS feature extends the existing HCCP 1+1 cable interface redundancy feature, where one cable interface is designated the working interface, and a second cable interface is the protect interface. The protect interface comes online only when the working interface fails. The N+1 Redundancy feature allows a single cable interface to act as the protect interface for up to 7 cable interfaces in the Cisco uBR10012 router, thereby significantly reducing the cost of providing redundant operation. The cable interface connections are made through the Cisco uBR-RFSW RF Switch.

Cisco IOS Release 12.2(4)BC1b supports N+1 Redundancy on the Cisco uBR10012 router only.

Note The N+1 Redundancy feature, used in conjunction with the Cisco uBR-RFSW RF switch, can now be used in DOCSIS 1.1 networks.

Note For complete information about the N+1 Redundancy feature, see the "N+1 Redundancy for the Cisco CMTS" chapter in the *Cisco CMTS Feature Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufgnpls1.htm

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.

No New Hardware Features in Release 12.2(4)BC1a

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

No New Software Features in Release 12.2(4)BC1a

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

New Hardware Features in Release 12.2(4)BC1

Cisco IOS Release 12.2(4)BC1 supports the following for new hardware features.

Cisco uBR10-SRP-OC12SML DPT WAN Card

Cisco IOS Release 12.2(4)BC1 supports the Cisco uBR10-SRP-OC12SML DPT WAN card on the Cisco uBR10012 universal broadband router. In this configuration, a DPT/OC12 Port Adapter is fitted into a processor board that has an NPE400 CPU complex using a R7000A processor. The Cisco IOS image for the DPT/OC12 WAN card runs on this processor. The WAN card processor is responsible for performing all SRP MAC processing and the drivers for the DPT/OC12 Port Adapter.

The DPT/OC12 functionality can be summarized as follows:

- Provides 2-fiber OC-12c dual ring connection (supports two 2-fiber rings) on the Cisco uBR10012. Capable of sending and receiving data and control on one or both rings simultaneously.
- Implements the Spatial Reuse Protocol (SRP ver 1) MAC to obtain fair shared access to the OC-12x rings.
- Provides ring wrap upon adjacent fiber or node failure.
- Supports single-mode intermediate-reach and long-reach capability for FCS. The software design does not exclude support for multimode capabilities.
- Provides interoperability with other routers supporting DPT OC12, including Cisco ubr7200, Cisco 7200 series, Cisco 7500 series, and GSR routers.
- Supports SONET DCC channel.
- Supports online insertion and removal (OIR) of the entire Port Adapter assembly.
- Supports interface with the PRE for packet forwarding (PRE does the routing and switching).

- Uses the backplane ethernet for exchange of CLI, SNMP, and general management messages with the PRE.
- Uses three front panel LEDs to indicate the state of the card (Power, Status and Maintenance LED).

Note Cisco IOS Release 12.2(4)BC1 does not support the CISCO-SRP-MIB.my MIB for the Cisco uBR10-SRP-OC12SML DPT WAN card.

New Software Feature in Release 12.2(4)BC1

Cisco IOS Release 12.2(4)BC1 includes support for the following new software features.

Support for the cable power Command

The **cable power** command provides a way to use the command-line interface (CLI) to manually power a cable interface line card on or off in the Cisco uBR10012 router. This command is typically not used during normal operations, but it can be used for lab, diagnostic, and troubleshooting purposes.

Using this command to first power off and then power on a card is functionally equivalent to performing an online insertion and removal (OIR) of the card. You can also use the LC Power off Status Reg and Line Card Presence Status Reg fields in the **show controllers clock-reference** command to determine whether a cable interface line card is actually present in the chassis and whether it has been powered on or off.

Note For full documentation on this command, and for important notes and limitations on its use, see the *Cisco Cable Modem Termination System Commands* chapter in the *Cisco Broadband Cable Command Reference Guide*.

New Hardware Features in Release 12.2(4)XF1

Cisco IOS Release 12.2(4)XF1 supports the following for new hardware features.

Cisco uBR-RFSW RF Switch

The Cisco uBR-RFSW RF Switch provides the physical cabling support for the N+1 Redundancy for the Cisco CMTS feature, which allows a single cable interface to act as the protect interface for up to 7 cable interfaces in the Cisco uBR10012 router, thereby significantly reducing the cost of providing redundant operation. The cable interface connections are made through the Cisco uBR-RFSW RF Switch, which provides the connections required for both upstream and downstream port redundancy.

Note For complete information about the Cisco uBR-RFSW RF Switch, see the documents in the *Cisco uBR-RFSW RF Switch* documentation directory on Cisco.com.

New Software Features in Release 12.2(4)XF1

Cisco IOS Release 12.2(4)XF1 includes support for the following new software features.

N+1 Redundancy for the Cisco CMTS

The N+1 Redundancy for the Cisco CMTS feature extends the existing HCCP 1+1 cable interface redundancy feature, where one cable interface is designated the working interface, and a second cable interface is the protect interface. The protect interface comes online only when the working interface fails.

The N+1 Redundancy feature allows a single cable interface to act as the protect interface for up to 7 cable interfaces in the Cisco uBR10012 router, thereby significantly reducing the cost of providing redundant operation. The cable interface connections are made through the Cisco uBR-RFSW RF Switch.

Note For complete information about the N+1 Redundancy feature, see the *N+1 Redundancy for the Cisco CMTS* chapter in the *Cisco CMTS Feature Guide*.

New Hardware Features in Release 12.2(4)XF

Cisco IOS Release 12.2(4)XF includes support for the following new hardware features.

Cisco uBR-LCP-MC16C Cable Interface Line Card

Cisco IOS Release 12.2(4)XF adds support for the Cisco uBR-LCP-MC16C cable interface line card, which is a combination of the Cisco uBR-LCP and Cisco uBR-MC16C line cards. The Cisco uBR-LCP card adapts the Cisco uBR-MC16C to the electrical requirements and form factor of the Cisco uBR10012 chassis.

The Cisco uBR-LCP-MC16C line card provides one downstream and six upstreams that support the DOCSIS (Annex B) 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.

The Cisco uBR10012 chassis supports a maximum of eight Cisco uBR-LCP-MC16C line cards. The Cisco uBR10012 chassis also supports the Cisco uBR-LCP-MC16C card along with any combination of the other supported cable interface line cards, up to a maximum of eight cards.

Note The Cisco uBR-LCP line processor card must be at revision 4.4 or greater and be using the boothelper image from Cisco IOS Release 12.2(2)XF1 or later to support the Cisco uBR-MC16C cable interface line card.

Cisco uBR-LCP-MC16E Cable Interface Line Card

Cisco IOS Release 12.2(4)XF adds support for the Cisco uBR-LCP-MC16E cable interface line card, which is a combination of the Cisco uBR-LCP and Cisco uBR-MC16E line cards. The Cisco uBR-LCP card adapts the Cisco uBR-MC16E to the electrical requirements and form factor of the Cisco uBR10012 chassis.

The Cisco uBR-LCP-MC16E cable interface line card provides one downstream and six upstreams that support the EuroDOCSIS (Annex A) standard. EuroDOCSIS 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 uBR10012 chassis supports a maximum of eight Cisco uBR-LCP-MC16E line cards. The Cisco uBR10012 chassis also supports the Cisco uBR-LCP-MC16E card along with any combination of the other supported cable interface line cards, up to a maximum of eight cards.

Note The Cisco uBR-LCP line processor card must be at revision 4.4 or greater and be using the boothelper image from Cisco IOS Release 12.2(2)XF1 or later to support the Cisco uBR-MC16E cable interface line card.

PRE1 Performance Routing Engine

Cisco IOS Release 12.2(4)XF adds support for the PRE1 Performance Routing Engine processor card on the Cisco uBR10012 router. The PRE1 module enhances the existing PRE module functionality by adding support for Error Checking and Correction (ECC) for all onboard memory, replacing the simpler parity error algorithm.

Where parity error detection can only detect errors, the ECC feature helps protect against processor downtime by correcting errors as well as detecting them. The PRE1 module can automatically correct single-bit errors as small as 1 bit per nibble, protecting the PRE1 module from memory corruption due to transient memory problems.

The ECC feature is also more sensitive and precise in detecting errors. The PRE1 module can detect an error in only 1 bit out of each 64-bit block. It can also detect errors in two, three, or four bits in each 64-bit block.

Cisco IOS Release 12.2(4)XF automatically enables the ECC feature on PRE1 modules. Two CLI commands are also enhanced to provide information about ECC operation:

- **show hardware pxf xcm**—Adds a display for the ECC counters for each PRE1 module. For the older PRE modules, this command shows the message “ECC is not supported for this revision.”
- **clear pxf xcm counters**—Adds support for clearing the ECC counters.

The **show version** command also indicates whether a PRE or PRE1 module is the active processor module.

Note The order number for the PRE1 module is UBR10-PRE1. The order number for a spare PRE1 module is UBR10-PRE1=.

DC PEM with Alarm Status Connector

Cisco IOS Release 12.2(4)XF supports the new model of the DC Power Entry Module (PEM), which is identical in form and function to the original DC PEM, except that the new model includes an RJ-45 connector on the front panel to connect to the power supply monitoring connector on the optional 2400-watt AC-input power shelf.

Note If you are not using the optional 2400-watt AC-input power shelf, both models of DC PEM are functionally identical.

New Software Feature in Release 12.2(4)XF

Cisco IOS Release 12.2(4)XF include supports for the following new software features.

Route Processor Redundancy Support

Cisco IOS Release 12.2(4)XF introduces support for Route Processor Redundancy (RPR) on the Cisco uBR10012 universal broadband router. The RPR feature enables the Cisco uBR10012 to use two PRE or PRE1 modules in a redundant configuration, so that if the primary PRE or PRE1 module fails or becomes inactive, the system automatically performs a *failover*, where the secondary PRE or PRE1 module takes over and assumes full responsibility for systems operations.

The RPR feature does not require a full reboot of the system to perform a failover. When the system is originally initialized, the secondary PRE or PRE1 module performs an abbreviated initialization routine—the module performs all self-checks and loads the Cisco IOS software, but instead of performing normal systems operations it begins monitoring the primary PRE module. If the secondary PRE or PRE1 module detects a failure in the primary module, it can quickly assume the primary responsibility for systems operations.

Support for the cable monitor Command

Cisco IOS Release 12.2(4)XF supports the **cable monitor** command, which allows an external LAN packet analyzer or other server to monitor inbound and outbound data packets for specific types of traffic sent between the Cisco CMTS and the cable modems on a cable interface. This feature enables the CMTS administrator to analyze traffic problems with customer data exchanges. For complete information on configuring and using this feature, see the *Cable Monitor for the Cisco CMTS* chapter in the *Cisco CMTS Feature Guide*, available on Cisco.com and the Customer Documentation CD-ROM.

No New Hardware Features in Release 12.2(2)XF1

Cisco IOS Release 12.2(2)XF1 does not include support for any new hardware features.

No New Software Feature in Release 12.2(2)XF1

Cisco IOS Release 12.2(2)XF1 does not include support for any new software features.

No New Hardware Features in Release 12.2(2)XF

Cisco IOS Release 12.2(2)XF does not include support for any new hardware features.

No New Software Feature in Release 12.2(2)XF

Cisco IOS Release 12.2(2)XF does not include support for any new software features.

No New Hardware Features in Release 12.2(1)XF1

Cisco IOS Release 12.2(1)XF1 does not include support for any new hardware features.

New Software Feature in Release 12.2(1)XF1

Cisco IOS Release 12.2(1)XF1 adds software support for DOCSIS Baseline Privacy Interface (BPI) encryption and authentication.

New Hardware Features in Release 12.2(1)XF

Cisco IOS Release 12.2(1)XF introduces the Cisco uBR10012 router chassis and the FRU components described in *Cisco uBR10000 Series Universal Broadband Router Hardware Installation Guide* and the *Field Replaceable Units (FRUs)* documents.

New Software Feature in Release 12.2(1)XF

Cisco IOS Release 12.2(1)XF introduces software support for the Cisco uBR10012 router, as described in the *Cisco uBR10000 Series Universal Broadband Router Software Configuration Guide*.

Limitations and Restrictions

The following limitations and restrictions apply to Cisco IOS Release 12.2(15)BC2i.

Load-balancing and N+1

When N+1 switchover occurs, load-balancing configurations do not carry over from Working to Protect interface(s). Therefore upstreams and downstreams do not balance cable modems on the Protect interface(s).

Cisco uBR-MC5X20S Cable Interface Line Card

The Cisco uBR10-MC5X20S cable interface line card introduced in Cisco IOS Release 12.2(11)BC3 has the following limitations and restrictions:

- When you change the symbol rate on the Cisco uBR10-MC5X20S cable interface line card, and then immediately use the **show controller cable upstream** command, you can see the notation, "US phy SNR_estimate - Unknown" for a brief period of time. Wait a minute and reissue the command to get an accurate signal-to-noise ratio (SNR) value.
- Occasionally, after the Cisco uBR10-MC5X20S cable interface line card is installed, when you issue the **show proc cpu** command, you see a CPU utilization value of 100% even when the card is not processing any traffic. This is due to a temporary timing readjustment and you can ignore the value. Reissue the command after a few minutes to get an accurate CPU utilization value.
- When fragmentation is not used and concatenation is enabled, which can result in packet sizes larger than 2KB, the Cisco uBR10-MC5X20S cable interface line card can drop packets. This is by design and you can avoid the problem by enabling fragmentation. Or if you disable fragmentation, then limit the maximum concatenation burst parameter to 2KB.
- The **show interface cable sid counter verbose** command always displays a value of 0 for concatenated packets, even when concatenation is enabled for cable modems on a Cisco uBR10-MC5X20S cable interface.
- Cisco IOS Release 12.2(11)BC3 and the Cisco uBR10-MC5X20S cable interface line card require the use of the Cisco PRE1 module in the Cisco uBR10012 universal broadband router. If you are using redundant processors, both processors must be Cisco PRE1 modules.
- The following software features are not supported for the Cisco uBR10-MC5X20S cable interface line card with Cisco IOS Release 12.2(15)BC2i:
  - Cable Monitor
  - Point-to-Point Protocol over Ethernet (PPPoE)

Note HCCP 1+1 and N+1 redundant configurations are not supported in releases prior to Cisco IOS Release 12.2(15)BC1.

- The Cisco uBR10-MC5X20S cable interface line card includes onboard spectrum analyzer hardware. However, card support for advanced spectrum management features on the Cisco uBR10-MC5X20S cable interface line card will commence with future Cisco IOS releases. Future advanced spectrum management support will include all features currently available with the Cisco uBR-LCP2-MC16S cable interface line card.

Note Prior to Cisco IOS Release 12.2(15)BC1 and the introduction of virtual interfaces, the configuration of the downstream and upstream ports was fixed into five domains.

Route Processor Redundancy Plus (RPR+)

The RPR+ feature introduced in Cisco IOS Release 12.2(11)BC3 has the following limitations and restrictions:

Console Port Usage After a PRE1 Module Switchover

When a primary PRE1 module fails, and the secondary PRE1 module becomes the primary PRE1 module, you must use the console port on the new primary PRE1 module to give Cisco IOS CLI commands and display statistics for the system. If you have connected your PC or terminal to the console port on a primary PRE1 module and a switchover occurs, you will no longer be able to access the console, and the display will read "Secondary console disabled."

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

External Management Stations

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

Flap Detection on WAN Interfaces During Switchover

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

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

Link States Reinitialized After Switchover

The synchronization of link states is not maintained between the Active Route Processor (RP) and Standby RP. Link states are re-initialized after switchover

MIB Variables Reinitialized After Switchover

All MIB variables are re-initialized following a switchover.

SNMP Not Supported During Switchover

SNMP persistence is not supported through a PRE1 switchover.

Telnet Sessions Disconnected During Switchover

A switchover automatically disconnects any Telnet sessions on the primary (failed) PRE1 module.

Encrypted Multicast Not Supported

Encrypted multicast broadcast is not supported during a PRE1 switchover.

Gigabit Ethernet Performance Limitations on Small Packets

On the Cisco uBR10012 router, processing small packets (64 bytes or fewer) limits a Gigabit Ethernet interface to approximately 80% of full line rate performance. Full performance is attained when the Gigabit Ethernet interface is processing packets that are 80 bytes or larger.

Downstream Rate-limiting Cannot Be Disabled

In Cisco IOS Release 12.2(11)BC2, you can no longer disable downstream rate-limiting on the Cisco uBR10012 router by using the **no cable downstream rate-limit** command. You can use the **cable downstream rate-limit** command to change the rate-limiting on the downstream ports, but you cannot disable downstream rate-limiting entirely.

Channel-width and Minislot Size

Cable modems can go offline if you manually change the channel-width on an upstream without also changing the minislot size to the corresponding value. This restriction applies more to DOCSIS 1.0 and older cable modems. See the following examples for the correct channel-width and minislot pairings:

```
cable upstream 0 channel-width 3200000
cable upstream 0 minislot 4

cable upstream 0 channel-width 1600000
cable upstream 0 minislot 8

cable upstream 0 channel-width 800000
cable upstream 0 minislot 16

cable upstream 0 channel-width 400000
cable upstream 0 minislot 32

cable upstream 0 channel-width 200000
cable upstream 0 minislot 64
```

Frame Relay Not Supported

- Frame Relay is not currently supported on any interfaces on the Cisco uBR10012 router.
- Although commands for Frame Relay support appear as part of the CLI on the Cisco uBR10012 router, Frame Relay operations are not supported on the network uplink WAN interface line cards.

N+1 Redundancy Limitations and Restrictions

PacketCable and N+1 Interoperation

PacketCable operations can be configured together with HCCP N+1 redundancy, but the PacketCable states are not synchronized between the Working and Protect interfaces. If a switchover occurs, existing voice calls continue. However when the user hangs up, PacketCable event messages are not generated because the Protect interface is not aware of the previous call states.

New voice calls can be made and proceed in the normal fashion.

Encrypted Multicast Not Supported

DOCSIS 1.1 N+1 Redundancy does not support encrypted multicast broadcasts across a line card switchover.

N+1 Redundancy and Cable Modem Compatibility

For a cable modem to be compatible with N+1 Redundancy support on the Cisco uBR10012, the cable modem must be DOCSIS 1.0 certified, so that it is able to tolerate disconnections from the coaxial cable network for five to fifteen seconds, without the cable modem going offline and reinitializing.

N+1 Redundancy and Configuring Static Multicast Groups

N+1 Redundancy on the uBR10012 is not supported when you are also configuring static multicast groups with the **ip igmp static-group** commands. If the static multicast groups are configured along with N+1 Redundancy, the PRE module may hang after a switchover. This limitation is described in caveat CSCdy11181.

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 uBR10012 universal broadband router supports 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 2600 series router, 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 uBR10012 router. They include both DOCSIS-specific MIBs and Cisco-specific enterprise MIBs. If your network management applications have not already been configured for the Cisco uBR10012 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.
- CISCO-ENTITY-VENDORTYPE-OID-MIB

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 10 shows the cable-specific MIBs that are supported on the Cisco uBR10012 universal broadband router. 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 10 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/sw-center/netmgmt/cmtk/mibs.shtml). Most MIBs are available in both SNMPv1 and SNMPv2 versions; the SNMPv1 versions have *V1SMI* as part of their filenames.

Note Cisco IOS Release 12.2(15)BC2i does not support the CISCO-SRP-MIB.my MIB for the Cisco uBR10-SRP-OC12SML DPT WAN card.

Table 10 Cable-Specific MIBs Supported on Cisco uBR10012 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 RFC1902.	12.2(1)XF1
SNMPv2-TC.my SNMPv2-TC-V1SMI.my	This module defines the textual conventions as specified in RFC1903.	12.2(1)XF1
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 RFC1907.	12.2(1)XF1
CISCO-SMI.my CISCO-SMI-V1SMI.my	This module specifies the SMI for Cisco's enterprise MIBs.	12.2(1)XF1
CISCO-TC.my CISCO-TC-V1SMI.my	This module defines the textual conventions used in Cisco's enterprise MIBs.	12.2(1)XF1
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 RFC2233.	12.2(1)XF1
DOCS-IF-MIB.my DOCS-IF-MIB-V1SMI.my	This module describes the DOCSIS-compliant Radio Frequency (RF) interfaces in CMs and the CMTS. This MIB has been released as an RFC2670.	12.2(1)XF1
DOCS-BPI-MIB.my DOCS-BPI-MIB-V1SMI.my	This module describes the attributes for the DOCSIS 1.0-specified Baseline Privacy Interface (BPI) on cable modems and the CMTS.	12.2(1)XF1
DOCS-BPI-PLUS-MIB.my[1] DOCS-BPI-PLUS-MIB-V1SMI.my	This module describes the attributes for the DOCSIS 1.1-specified Baseline Privacy Interface Plus (BPI+) on CMs and the CMTS. This is revision 05 of the MIB. **Note** In DOCSIS 1.1 operation, this MIB replaces the DOCSIS 1.0 version, DOCS-BPI-MIB.	12.2(1)XF1
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.	12.2(1)XF1
CISCO-CABLE-SPECTRUM-MIB.my CISCO-CABLE-SPECTRUM-MIB-V1SMI.my	This module describes the spectrum management and flap list attributes. **Note** The Cisco uBR10012 router supports only the flap list attributes in this MIB.	12.2(2)XF1
DOCS-QOS-MIB.my[1] DOCS-QOS-MIB-V1SMI.my	This module describes the quality of service (QoS) attributes. This is revision 04 of the MIB.	12.2(2)XF1

Table 10 Cable-Specific MIBs Supported on Cisco uBR10012 Routers (continued)

MIB Filename	Description	Introduced in Release
IGMP-MIB (RFC2933)[1]	This module describes the IGMP protocol attributes, as defined in RFC2933.	12.2(2)XF1
DOCS-IF-EXT-MIB.my[1]	This is the extension of module of the RFC2670 (DOCS-IF-MIB).	12.2(2)XF1

1. These MIBs are in draft form. They have not yet been finalized by the DOCSIS committee and are subject to change with future releases.

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 11.

Table 11 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
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 11 represent feature sets that are not supported on Cisco uBR10012 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 selected 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.* This document lists severity 1 and severity 2 caveats and only selected severity 3 caveats, 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 13 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 12 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 13 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 13 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 38 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 14 Closed and Resolved Caveats for Release 12.2(15)BC2g

Caveat ID Number	Description
CSCef14781	The PRE may report the error below during a PRE switchover: `%UBR10K-3-QUEUEFULL: Unable to enqueue since the queue is full` There are no known workarounds.
CSCef86161	Traffic recovery after LC switchover may be inconsistent if BPI+ is configured and the default TEK lifetime/gracetime is changed. There are no known workarounds.
CSCef93215	A router that is configured for OSPF may reload unexpectedly and reference the “ospf_build_one_paced_update” process. This 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.
CSCeg80463	After issuing the following command “no ip vrf ISP-V1” a traceback is observed and the PRE1 unexpectedly reloads. There are no known workarounds.

CSCeh00967	A uBR10012 router running 12.2(15)BC2d can display different information in the output of “show cable spectrum” depending if this is done directly as a command, or if it is called through the list of command executed by “sh tech”.
	This issue occur with cable spectrum-group configured on different cable interfaces. In addition, the total number of interface on the system needs to exceed 144 example:
	`On RP of uBR10K there are 5 * 8 = 40 interfaces`
	`With 4 upstreams for each interface we have a total of  40 * 4 = 160`
	Workaround: Look at the output of “sh tech”.

Table 14 Closed and Resolved Caveats for Release 12.2(15)BC2g (continued)

Caveat ID Number	Description
CSCeh01845	This issue is observed with both fragmentation and concatenation are enabled. Workaround: Disable fragmentation by configuring “no cable upstream n fragmentation”.
CSCeh20178	Stabilize 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.
CSCeh37712	This fix enables the LCHUNG process on the uBR10012 RP. This process will power cycle any hung cable line card. There is an exec command “auto-clc-hang-reset on|off” which can disable or enable the polling. The default will be enable. There are no known workarounds.
CSCeh42526	The LCHUNG process on uBR10012 router performs a line card reset when a hang line card is detected. Because of a problem with a FPGA on the MC520, which can cause the line card to hang, the LCHUNG process should power cycle the line card to get around the FPGA problem. There are no known workarounds.
CSCeh43502	An unexpectedly reloads occurs while modifying/applying mcast access list This issue occurs with a failure in creation of multicast service flow first, followed by modifying/applying of macst access list There are no known workarounds.
CSCsa47427	With dynamic secret enabled, if ALL conditions described below are true, modems may get stuck in init(o) state and fail to register. The conditions are: 1. Each modem gets its own config file (for e.g. as when BACC is used for provisioning) 2. The CM config files are large (greater an 1024 bytes in size) 3. Large number are trying to connect to the CMTS 4. The RP CPU is high (close to 100%) Workaround: Reduce the number of modems trying to connect to the CMTS at the same time. This includes increasing insertion interval & ranging backoffs, shutting down interfaces or upstreams.
CSCsa54614	The problem is that All cms connected to c8/1/1 up1 stayed offline or init(r1). When checking the phydump during the problem, TRLRSTAT error occurred and “UBR10000-4-BADTXOFFSET: Bad timing offset” was displayed. During the problem, UCD and slots counts were incremented during the problem. Workaround: After shut/no shut of the upstream port, all cms came online.

Table 14 Closed and Resolved Caveats for Release 12.2(15)BC2g (continued)

Caveat ID Number	Description
CSCsa63951	Poor performance may be observed such as VoIP latency, dropped packets, uncorr FEC errors under the **sh cab hop** command, T3 timeouts from the modem, etc. This is caused by dynamic map advance being calculated based on a wrong time offset from non-compliant DOCSIS modems. The current IOS helps mitigate this by allowing a "cap" to be configured and also the time offset in the **sh controller** command to be updated every 15 minutes. This 15 minute update is inconsistent and is not working or hanging. This issue occurs when using dynamic map-advance and modems misbehave by caching their time offsets when they reboot, the map-advance for the entire US port can be affected and have poor performance for all modems on that US port. Workaround: Configure a realistic map advance “cap”. Example, if the highest time offset during normal operation on a particular US is 5000, then the following command can be used, cab map-advance dynamic 1000 500. The safety amount of 1000 is the default, but using a "cap" of 500 will limit the time offset to a cap of 500*64/6.25 = 5120.

CSCsa69875	With arp reply filter enabled, a modem will show as “online” from “show cable modem” but may not have an arp entry. “show ip arp <modem ip addr>” will be empty.
	
	This issue occurs when the cable interface command “cable arp filter reply-accept <packets> <time window>” is present. Virus activity is high on the CMTS. There is a Linksys router with faulty firmware behind the modem. The fault is that the LInksys sends an arp reply to all arp requests. This problem is described in the Cisco Arp Filter documentation. Potential OUIs that can be faulty are:
	
	`00-06-25 (hex)The Linksys Group, Inc.`
	`00-0C-41 (hex)The Linksys Group, Inc.`
	`00-0F-66 (hex)Cisco-Linksys`
	`00-12-17 (hex)Cisco-Linksys, LLC`
	
	High virus activity causes the CMTS to send many broadcast arp requests which in turn causes the Linksys to send many arp replies. This can statistically cause the periodic arp refresh of the arp entry for the modem to fail.
	
	Workaround: The correct solution is to follow the procedure in the ARP Filter documentation to isolate the Linksys devices and have the end user upgrade the firmware from site:
	
	http://www.linksys.com/Download/
	
	Alternative workaround: Disable the arp filter on the interface having modems with no arp entry. This will unfortunately cause significant arp traffic to be received on the RP or NPE.
	
	Launch an effort to use the Arp Filter documentation to isolate and upgrade the Linksys devices with repaired firmware.
	
	Launch an effort to have end users run anti-virus software.

Table 14 Closed and Resolved Caveats for Release 12.2(15)BC2g (continued)

Caveat ID Number	Description

CSCsa76715	Frequent SNMP queries of the ubr10k arp table by ipNetToMediaTable or atEntry will result in high cpu usage by the SNMP ENGINE process, upwards to 80%.
	
	Note that SNMP will use as much CPU as it can get and that is expected. If other medium priority processes need CPU, SNMP will gracefully share the CPU with those processes. The problem is more so that SNMP will continuously use high CPU indefinitely instead of using it for a few minutes to satisfy the lengthy ipNetToMediaTable query.
	
	Queries that create high CPU are for atEntry and ipNetToMediaTable. This can be triggered by network tools such as OpenView or CiscoWorks doing auto-discovery of the network. If the query does not complete in a certain time window, it appears that the tools will retry the query. This keeps the CPU usage at a high level constantly as opposed to a high level for just a 5 to 10 minute period.
	
	Although SNMP will usually appear to use high CPU, this problem was made worse on the 12.2(15)BC2 train at 12.2(15)BC2e and the 12.3(9a)BC train from its first release by fixing CSCeg24134. Note that 12.2(15)BC2d has low CPU because due to a bug introduced by CSCef04614, the result set for the query is a fraction of what it should be. When CSCeg24134 was fixed, it greatly increased the query time and started the abort/retry problem with the snmp tools.
	
	Workarounds:
	
	1) If an extreme problem, turn off querying. If snmp servers cannot be isolated, setup an ACL on port 161.
	
	2) Allow for a longer query time. If the querying tool is configurable, adjust configuration so that the atEntry and ipNetToMediaTable queries have more time to finish. As a guide, a test system with 12,000 arp table entries shows that the ipNetToMediaTable query takes 12 minutes to complete with 12.3(9)BC2. After this bug fix, CSCsa76715, it takes 7 minutes 30 seconds to complete.
	
	3) Exclude the ipNetToMediaTable from querying. The following config will achieve this:
	
	`snmp-server view noarp ipNetToMediaEntry excluded`
	`snmp-server view noarp iso include`
	`snmp-server community public view noarp ro`
	
	The impact of 3 is that there will be no results returned to the tool.
	
	4) Exclude 3 of the 4 subtables of ipNetToMediaTable. This will cut the query time by 75%:
	
	`ipNetToMediaTable is comprised of 4 tables:`
	`ipNetToMediaIfIndex aka ipNetToMediaEntry.1`
	`ipNetToMediaPhysAddress aka ipNetToMediaEntry.2`
	`ipNetToMediaNetAddress aka ipNetToMediaEntry.3`
	`ipNetToMediaType aka ipNetToMediaEntry.4`

Table 14 Closed and Resolved Caveats for Release 12.2(15)BC2g (continued)

Caveat ID Number	Description

	Querying each of these tables takes equal time, therefore if the tool's needs are satisfied by querying just one of the four tables, the total query time will be approximately 25% than without such a config. The ipNetToMediaPhysAddress is probably the most useful table to query since it includes the interface index, the IP address, and the mac address of the arp entry.
	Example:
	`ipNetToMediaPhysAddress.2.10.11.1.15 = 00 05 00 e5 35 d4`
	A sample configuration that includes just ipNetToMediaPhysAddress is:
	`snmp-server view noarp ipNetToMediaEntry.1 excluded`
	`snmp-server view noarp ipNetToMediaEntry.3 excluded`
	`snmp-server view noarp ipNetToMediaEntry.4 excluded`
	`snmp-server view noarp iso include`
	`snmp-server community  public view noarp ro`
	Such a configuration will take a 12 minute query time down to 3 minutes which may let the querying tool finish its discovery and avoid an abort/retry cycle.
	For reference, here is the sample output showing how one arp entry creates four results records from the ipNetToMediaTable query:
	`ipNetToMediaIfIndex.7.192.168.81.1 = 7`
	`ipNetToMediaPhysAddress.7.192.168.81.1 = 00 05 00 e5 36 10`
	`ipNetToMediaNetAddress.7.192.168.81.1 = 192.168.81.1`
	`ipNetToMediaType.7.192.168.81.1 = static(4)`
	One can see that merely excluding the ipNetToMediaType table, which shows if the arp entry is static or dynamic, will cut the query time by 25%.

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 38 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 15 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.
CSCed85422	Upconverter of UBR10-MC5X20S-D works with different rf-power value being configured on running-configuration. After booting up without saving changes for rf-power value. Workaround: Re-configure appropriate rf-power value.

CSCed89010	The **hccp reverttime** command does not work correctly. Although configured, it reverts back just after suspend timer (WaitToRestore) comes to zero with following messages:
	`SYS-3-TIMERNEG: Cannot start timer (0x65720F10) with nega tive offset (-362867296).`
	`-Process= "HCCP_CTRL", ipl= 0, pid= 156`
	`-Traceback= 60540674 6053DD5C 6033F0CC 60340E34 60342B90 60343BA8`
	This issue occurs when setting up a large number like “65535” as “hccp reverttime”.
	Workaround: Using a revert timer value less than or equal to 35791 minutes. Or, using **no hccp revertive** command.

CSCee24856	A 520 line card may unexpectedly reload because of a bad JIB header packet, which causes the code to index to an invalid IDB. The unexpected reload is then caused by a reference to the IDB. Workaround: Add JIB header checking code to the JIB is receive routine for the low priority queue.
CSCee44374	If the CLC unexpectedly reloads shortly after being booted, an “uninitialized timer” message like the following: `%SYS-3-MGDTIMER: Uninitialized timer, timer stop in hccp code shows up.` There are no known workarounds.

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

Caveat ID Number	Description
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
CSCef23733	Redundant PRE may continuously reload on bootup. This condition can occur if a PRE switch over occurred since loading the previous version of software and during the previous load of software on the currently active/previously redundant PRE some linecards were in the process of booting. If this condition persists a reload of both PRE's is necessary. There are no known workarounds.
CSCef23937	N+1 switchover events will NOT work properly in a setup which does NOT have RF switch between the Working and Protect LC. Workaround: Have a dummy config line in the HCCP config for RF switch, even if there is no RF switch physically present.

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

Caveat ID Number	Description
CSCef44225	A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt). These attacks, which only affect sessions terminating or originating on a device itself, can be of three types: 1. Attacks that use ICMP "hard" error messages 2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks 3. Attacks that use ICMP "source quench" messages Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type. Multiple Cisco products are affected by the attacks described in this Internet draft. Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml. The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

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

Caveat ID Number	Description
CSCef44699	A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt). These attacks, which only affect sessions terminating or originating on a device itself, can be of three types: 1. Attacks that use ICMP "hard" error messages 2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks 3. Attacks that use ICMP "source quench" messages Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type. Multiple Cisco products are affected by the attacks described in this Internet draft. Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml. The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

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

Caveat ID Number	Description
CSCef60659	A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt). These attacks, which only affect sessions terminating or originating on a device itself, can be of three types: 1. Attacks that use ICMP "hard" error messages 2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks 3. Attacks that use ICMP "source quench" messages Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type. Multiple Cisco products are affected by the attacks described in this Internet draft. Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml. The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.
CSCef75363	After a N+1 switch over, the ARP entry for CPE devices may not be automatically created until subscriber traffic forces an ARP refresh. This may add a small delay to traffic recovery during the ARP request/response exchange. Workaround. CPE traffic will recover without any user intervention.
CSCef79820	The mac-scheduler is not cleared properly with non packetcable call. As a result, the mac-scheduler is full little by little after every a call and can not make a call due to DSA_MULTIPLE_ERRORS. This issue occurs when the docsis-mode is tdma-atdma (mix) mode in Cisco IOS software version 12.2(15)BC2a later. Workaround: Use "cable upstream x shutdown" and "no cable upstream x shutdown"

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

Caveat ID Number	Description
CSCef87118	In version 12.2(15)BC2c, the DHCPD Receive process may hold memory when DMIC is used. When DMIC is used, about 368 bytes of memory is lost on the CMTS for each config file used for the modem. This loss would keep growing till the system runs out of memory. There are no known workarounds.
CSCef89820	The Line card unexpectedly reloads during N+1 switchover. There are no known workarounds.
CSCeg07988	When using the SNMP set command to change a modulation profile through the docsIfCmtsModulationEntry the CMTS will accept the change on the MIBs but will not apply it. If SNMP get is done on it, it will show the update Val, it also updating the modulation profile in the CMTS CLI but the modems will not apply it to the modems. The CMTS does not send the Update UCD to the CM. When they are forcing the UCD update by CLI using the Command: cable modulation-profile X the CMTS accepts it and sends the new UCD to CM. This issue was observed on 12.2(15)BC2b on a uBR10012 router with a PRE1 and a mc520 card. Workaround: Use the CLI to change the modulation profiles.
CSCeg12481	DHCP Proxy feature configured on the Cable Modem is not supported by CMTS. The CMTS is dropping the DHCPOFFER from the DHCP server if the ip address assigned to a CPE does not belong to any directly connected interface. This problem is being triggered by CSCee84392. This message is the one that could be seen if DHCP debug is enabled: `Oct 23 02:51:28.252 GMT: DHCPGLEAN hwidb/idb Cable6/1/0/NULL not found for MAC 0007.0e06.560c Ipaddr 10.1.1.220 Giaddr 10.1.1.1 DHCP type 2 dropped` There are no known workarounds.

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

Caveat ID Number	Description

CSCeg14041	A Cisco uBR100012 router with PRE1-RP processor running 12.2(15)BC2d may unexpectedly reload due to bus error after an interface flapping. The sequence and error message would be seen as follows:
	`UTC2: %UBR10000-6-CMMOVED: Cable modem <MAC_address> has been moved from interface Cable8/1/0 to interface Cable8/1/3.`
	`Unexpected exception, CPU signal 10, PC = 0x6013AFA8`
	`-Traceback= 6013AFA8 6021D5D4 601F8B9C 602BB304 602BB848 602E67AC 602E6CE4 602E6D70 602E7AE4`
	The unexpected reload is due to memory corruption.
	Workaround: Do not issue CLI "clear cable flap-list all"

CSCeg23455	The PXF queue allocation fails due to insufficient queue resources, although there are only small number of queues on the interface. Further investigation found that the problem was caused by stale secondary (dynamic) service flows on the RP. The source of this problem in unclear, but it is likely to have been induced by PRE switchover event. Workaround: Clear the cable modems to which the stale service flow belongs.
CSCeg30130	In CSCee32618, the user got a traceback following a "No current_if_info" message. The DDTS was unreproducible but I added some additional print outs in case this happened again. There are no known workarounds.
CSCeg36445	A Cisco Universal Broadband Router may reload unexpectedly as a result of its memory getting corrupted. This will cause a switch-over to the Standby PRE. There are no known workarounds.
CSCeg42335	A Cisco uBR10012(Pre1) Broadband Router may experience a packet latency/loss issue on cable interfaces when "cable source-verify [dhcp]" is configured. This issue is observed on a Cisco uBR10012(Pre1) Broadband Router that run Cisco IOS Release 12.2(15)BC02 when the cable interfaces have "cable source-verify [dhcp]" configured. The issue may occur also in other releases. Workaround: Turn off source verify, reload the box then shutdown all the cable interfaces (or all the cable bundle master interfaces) and then bring them up one by one. Micro reload pxf and Pxf switchover.

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

Caveat ID Number	Description

CSCeg44108	A Cisco uBR-10000 family router may trigger a PXF processor unexpected reload.
	
	A large access-list must be applied on a Cable interface. The unexpected reload often happens shortly after cable modems are coming online and requesting their ip address using DHCP, or when broadcast traffic is sent to the Cable interface, or if the access-list is modified.
	
	The router will log the following messages:
	
	`%PXF-2-FAULT: T1 SW Exception: CPU[t1r2c1] 0x00000680 at 0x0C8D LR 0x090A`
	`%PXF-2-FAULT: T1 Exception summary: CPU[t1r2c1] Stat=0x00000003 HW=0x00000000 LB=0x00000000 SW=0x00000680`
	
	The PXF processor will resume operating, but may unexpectedly reload again in a cycle until the condition has been cleared.
	
	The unexpected reload is observed only when a split ACL is in use. Splits in ACLs can be observed with “show pxf cpu access-list security”.
	
	Workaround: Use a smaller ACL if possible. When modifying the access-list, detach it from the Cable interface beforehand and re-attach it when done.

CSCeg55961	For the entPhysicalName need to display the type of PRE as well along with the interface name. So, basically it needs to specify whether the interface belongs to the active PRE or the standby PRE.
	
	Currently the output displays the following:
	
	`entPhysicalName.29 = FastEthernet0/0/0`
	
	It needs to be changed to:
	
	`entPhysicalName.29 = PRE_X:FastEthernet0/0/0`
	
	Whereas “X” may be A or B. At any given time, either “A” or “B” would be Active or standby.
	
	There are no known workarounds.

CSCeg56960	The following occurs on the linecard when a PRE switchover happens:
	
	`SLOT 5/0: Dec 15 15:13:26.445 UTC: %REQGRP-3-SYSCALL: System call for command 2 (slot5/0) : Nonblocking req`
	`uest failed  (Cause: internal error)`
	`-Traceback= 60460610 604776C8 6047C89C 6047C910 6044A778 6044A87C 602C16D8`
	
	This issue occurs if all ipc traffic is not properly cleared.
	
	There are no known workarounds.

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

Caveat ID Number	Description
CSCeg71922	One or more linecards cards resets every 49 days. The exact interval is 7 weeks, 0 days, 17 hours, 2 minutes, 47 seconds (based on the rollover of a 32-bit 1 millisecond timer). A crashinfo file is left on the linecard with CPU Hog messages from the "CMTS Mac Timer" process, followed by a watchdog reset. It is a matter of probability as to whether or not the bug will be seen. If there is only 1 call up at the rollover time with a service flow with an activity timer, it has a 1 in 50 chance of crashing. The probability goes up with more calls in place. This issue occurs under the following conditions: – Linecard must have been up for 49 days – Service flows must have a non-zero activity timer – Packetcable configurations are more vulnerable than pure data configurations because voice service flows typically use activity timers. This issue has been observed on uBR10012 MC5X20 linecards, but any cable configuration, including the uBR7246VXR router, that uses service flow activity timers is vulnerable. Workaround: There is no perfect known workaround. However, the following are possibilities: – Set the service flow activity timer to zero a few hours before the clock will rollover. Reenable the activity timer after the rollover. – Check the uptime of the cards in the system, schedule a card reload prior to the rollover. – If N+1 is configured: switch a cards to the redundant card, reload the working card and then revert. Repeat for all cards approaching the 49 day rollover point. Note that the up time of a linecard can be seen with the **show diag** command.
CSCin80987	In a HA enabled CMTS if, a "clear cable modem" CLI is invoked and the CMTS any time later performs a PRE switchover and qos profile reference counts on the standby PRE will be completely wrong. This causes the qos profile deletion/addition behavior to be completely wrong after the switchover for all times to come. There are no known workarounds.
CSCin84603	Executing the **no debug all** command or the **undebug all** command can result in the following error message, along with a traceback: `%SCHED-7-WATCH: Attempt to enqueue uninitialized watched queue (address 0).` This issue occurs only when an SRP/OC-12 line card is installed in the CMTS. There are no known workarounds.

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

Caveat ID Number	Description
CSCin87306	The linecard unexpectedly reloads or shows traceback with alignment errors at time of PRE switchover. This issue occurs when redundant PREs are on a uBR10012. This issue does not apply to uBR7246 and is specific to the 12.2(15)BC2 release train. There are no known workarounds.
CSCsa59600	A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt). These attacks, which only affect sessions terminating or originating on a device itself, can be of three types: 1. Attacks that use ICMP "hard" error messages 2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks 3. Attacks that use ICMP "source quench" messages Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type. Multiple Cisco products are affected by the attacks described in this Internet draft. Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml. The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

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 38 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 16 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.
CSCed53225	Due to excessive memory fragmentation, a call to malloc fails even though available free memory may be greater than the requested size. There are no known workarounds.
CSCed87992	Low bandwidth downstream service flows can get more than the configured max_rate if the packet size in the flow is large. Workaround: Configure max_rate to be greater than 100kbps
CSCee60254	The ifHCInOctets (.1.3.6.1.2.1.31.1.1.1.6) counters are roo high for the gigabit interfaces on the UBR10000. This issue is seen when 12.2(15)BC2 is the current IOS version on the UBR. There are no known workarounds.

Table 16 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCee79463	The system may sometimes unexpectedly reload when the following messages flood the screen: `*Jun 8 17:40:15.923: %UBR10000-3-AUTH_INVALID_MESSAGE_AUTHENTICATION_FAILURE: <132>CMTS[DOCSIS]:<66030207> Auth Invalid - Message(Key Request) Authentication Failure . CM Mac Addr <0000.39ef.4a55> *Jun 8 17:40:31.083: %UBR10000-3-AUTH_INVALID_INVALID_KEY_SEQUENCE_NUMBER: <132>CMTS[DOCSIS]:<66030206> Auth Invalid - Invalid Key Sequence Number. CM Mac Addr <0000.3979.c454> *Jun 8 17:40:31.087: %UBR10000-3-AUTH_INVALID_MESSAGE_AUTHENTICATION_FAILURE: <132>CMTS[DOCSIS]:<66030207> Auth Invalid - Message(Key Request) Authentication Failure . CM Mac Addr <0000.3979.c454> *Jun 8 17:42:05.347: %UBR10000-3-INVALIDSIDPOSITION: Invalid SID (81) position for interface Cable8/1/0: CM 0007.0e03.38c5:Is used by CM 0000.0000.0000 SFID 0 SID 0. SID container info: start 81 end 54 -Traceback= 602C8110 602C8310 602C8B6C 602B5870 6035124C 605538E8 605538CC *Jun 8 17:42:45.363: %UBR10000-3-INVALIDSIDPOSITION: Invalid SID (81) position for interface Cable8/1/0: CM 0007.0e03.38c5:Is used by CM 0000.0000.0000 SFID 0 SID 0. SID container info: start 81 end 54 -Traceback= 602C8110 602C8310 602C8B6C 602B5870 6035124C 605538E8 605538CC CMTS-R7264#` There are no known workarounds.
CSCee85372	A traceback is observed since CM might have been removed from the flaplist while ccsFlapList query was running. Code has been added to avoid this traceback. There are no known workarounds.
CSCee93770	When modems simultaneously go offline on multiple line cards, the N+1 protocol may get into an inconsistent state. Modems cannot come online and the system does not recover. Some interfaces remain in an Updown Down state and modems can never come back online. Workaround: Hardware Module reset the Protect line card. Alternative workaround: Use shut/no shut on the non-functional interfaces

Table 16 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCef04085	After a N+1 switchover event, traffic modem counters are not updated while the modem is active on the Protect line card. There are no known workarounds.
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.
CSCef18997	Data transmission rate in a downstream direction for 256QAM modulation takes place with higher rate than configured in a cable modem profile. This can be observed with following CMTS commands: **show interface cable service-flow verbose** **show cable modem qos verbose** This has been noticed on MC16E and MC520U cards with FTP and UDP traffic. This issue is specific to Annex A and has not been noticed with 64QAM. There are no known workarounds.
CSCef24484	Cable modems are associated to wrong sub-interface in a MPLS VPN setup. This issue occurs when 2 DHCP server are defined/reachable from each sub-interfaces networks Workaround: Clear cable modem xxxx.xxxxx.xxxx del.
CSCef27859	This code improves the modem bring-up performance for a uBR10012 CMTS. This CMTS has much higher number of cable modems on it compared to the ubr7200 and that is why this code is being committed to take care of the higher modem count. There are no known workarounds.
CSCef31956	This caveat improves reverse arp lookup on the CMTS for modem bring-up. There are no known workarounds.

Table 16 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCef35392	All Cable Modems on an unspecified DS of an MC5X20U card become offline after hccp switchover and stay in the "offline" state. A "show controller cable <x/y/z>" shows "No MAP buffer" incrementing and the "UCD Count" for each upstream stuck. This issue is observed on a HCCP N+1 redundancy with Cisco uBR10-MC5X20U Cisco IOS software version 12.2(15)BC2b. Workaround: Reset the LC by "hw-module subslot x/y reset".

CSCef35754	IPC communications with a cable linecard fails. The user will see a recoverable ironbus fault followed by an IPC failure. Modems will eventually go offline and new modems will not be able to come online. The card will not be configurable:
	`Jul 21 02:08:56.212: %C10KEVENTMGR-1-IRONBUS_FAULT: Ironbus Event 5/0 - <Software-Initiated Event>, Restarting Ironbus`
	`Jul 21 02:08:56.203:  C10K_API_CMD_BARIUM_DISABLE command`
	`SLOT 5/0: Jul 21 02:08:56.227: %IPCGRP-6-BARENBDISAB: Barium interface disabled`
	`Jul 21 02:08:56.276: %C10KEVENTMGR-1-IRONBUS_SUCCESS: Ironbus Event 5/0 - <Software-Initiated Event>, Restart Successful`
	`Jul 21 02:08:56.231:  C10K_API_CMD_BARIUM_ENABLE command`
	`SLOT 5/0: Jul 21 02:09:29.195: %REQGRP-3-SYSCALL: System call for command 103 (slot6/0) : ipc_send_message failed (Cause: timeout)`
	`-Traceback= 60456A38 60457A98 60458084`
	`%No response from slot 5/0. Command aborted`
	A recoverable ironbus fault must occur on a cable line card subslot. IPC will fail if HCCP is or is not configured. Note that if two ironbus faults occur within 4 seconds, the subslot will be reset and the IPC connection will be recovered.
	Workaround: Reset the subslot that had the ironbus fault and the IPC connection to the linecard will be recovered.

CSCef42509	A uBR10012 running IOS 12.2(15)BC2b may reload due to bus error when error messages related to the environment are being logged with logging count enabled. For example: `%CI-3-CORETEMPMINOR: Core temperature minor limit exceeded (router#)logging count` Workaround: Configure "no logging count".
CSCef42849	In a PRE-1 and PRE-2, a timing violation occurs in the third-party vendor temperature sensor, causing the temperature reading to fail. This issue is observed in a Cisco 10000 series PRE-1 and PRE-2. Old-type temperature sensors are not effected. There are no known workarounds.

Table 16 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCef42977	Under heavy loads (around 500 kpps), the uBR10012 PXF can stop de-queuing packets from the low priority queues (default data queues). Workaround: The issue can be rectified by a PXF reload (microcode reload pxf).
CSCef43462	Unable to obtain SNMP MIB info correctly after PRE switchover, but is able to get ifDescr info correctly. However, some interface info are missing. This issue is observed on PRE redundancy with Cisco uBR10012 Cisco IOS software version 12.2(15)BC2b and 12.2(15)BC2c. Workaround: Reload PRE or the CLI “cable upstream max-ports...” would force the PRE to download the snmpinfo to CLC automatically.

CSCef44517	Immediately after booting up, a PRE-1 may unexpectedly reload with the following error:
	
	`%ERR-1-GT64120 (PCI-1): Fatal error, PCI retry counter expired`
	`GT=0xB4000000,`
	`cause=0x00001000,`
	`mask=0x00D01D00, real_cause=0x00001000`
	`bus_err_high=0x00000000,`
	`bus_err_low=0x00000000,`
	`addr_decode_err=0x00000470`
	
	The fault is limited to PRE-1 version 08 with Texas Instrument PCI bridge chips. This version can be identified by the Top Assy. Part Number visually (on the box) or in the show chassis CLI command:
	
	`Top Assy. Part Number : 800-17437-08`
	`^^^`
	
	Workaround: Upgrade IOS to 12.2(15)BC1e or higher.
	
	Alternative workaround: Upgrade IOS to 12.2(15)BC2d or higher.

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

Caveat ID Number	Description
CSCef49148	On the uBR10012 router, after configuring both the primary shared secret and the secondary shared secret on cable interfaces using the commands **cable shared-secret** and **cable shared-secondary-secret**, and the length of the secondary shared secret is longer than the primary, the cable line card (MC28C, MC5x20) may unexpectedly reload. There are no known workarounds.
CSCef49769	The 2x8 LC on the uBR10012 router can run very high CPU utilization for moderate amounts of upstream traffic. LCP1 is more susceptible than LCP2 due to lower base CPU performance. The 5x20 LC is not affected by this issue. This can cause box-wide issues as the LC throttles the PXF severely. Workarounds: Reduce load on the affect linecard by moving CMs to a different LC. If you have an LCP1 based 2x8 linecard, replace with LCP2 Replace 2x8 linecard with 5x20 linecard.
CSCef52235	uBR10012 router running either 12.2(15)BC2c or 12.2(15)BC1b will run into the following issues when a 2x8 LC is running at 100% CPU: 1. No telnet access, only the console port works. 2. Modems that are online cannot come back online, the get stuck in init(rc). 3. Message that is being seen when the CMTS becomes unreachable: `%C10KEVENTMGR-1-MINOR_FAULT: PXF DMA Full OCQ Wait Error` 4. Traffic slowing down for all the linecards, especially the backhaul interfaces The issue was seen on a uBR10012 router with 16,000 CMs. Workaround: Reduce load on the LC running at 100% CPU. Alternative workaround: Reload the PXF microcode.
CSCef54096	A uBR10012 router may unexpectedly reload due to IP INPUT process. There are no known workarounds.
CSCef56516	SNR values can lower then expected with MC520U card. The issue is observed if virtual connectors 16,17,18,19 are used. There are no known workarounds.
CSCef57375	On ubr7246VXR CMTS router, when MC28U card is configured as cable bundle slave and multicast static-group is configured on master on start-up configuration, after reload, the MC28U card interface fails to populate its multicast bundle entries to the cable bundle forwarding table. There are no known workarounds.
CSCef60926	In a 1.0+ redundant environment, if a switchover is issued using the **hccp x switch y** command, new downstream dynamic service flows are not established on all new call attempts through protect card. There are no known workarounds.

Table 16 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCef64537	The **HCCP unlock** command causes a CMTS to unexpectedly reload intermittently. There are no known workarounds.
CSCef69368	When toaster VTMS receives excessive OCQ flow offs from a linecard of to-rp link, it can cause severe performance degradation of VTMS. In worst cases, it can even lockup the timing wheel causing VTMS not to service any linecard. This issue occurs in excessive OCQ flow offs from linecard, such as in the presence of link oversubsrcription. There are no known workarounds.
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.
CSCef78292	CPUHOG traceback appears on the RP console during switchover. There are no known workarounds.
CSCef83416	After a switchover to the Protect LC, new BPI/PHS modems coming online on the Protect LC may not be pingable nor can user traffic be sent to them. This issue occurs in a 2+1 or a larger system. It does not occur in a 1+1 system. Workaround: Disable BPI/PHS.
CSCef85824	The router would unexpectedly reload as a result of the CLI commands: **show tech** **show pxf cpu queue <cable interface>** **show cr10k <cable interface> queue be** **show cr10k <cable interface> queue ll** **show cr10k <cable interface> queue cir** The memory allocation scheme changed from standard malloc to chunks. This resulted in a mismatch of memory management routines: `chunk_lock to be used in place of mem_lock.` There are no known workarounds.

Table 16 Closed and Resolved Caveats for Release 12.2(15)BC2e (continued)

Caveat ID Number	Description
CSCin78666	While performing a MIB walk with a fully loaded CMTS, the mib walk may get into loop with the object “docsQosParamSetServiceClassName”. There are no known workarounds.
CSCin82115	If the UGS docsis1.1 config file is provisioned to the Toshiba modem with BPI+ enabled, traffic may get stuck after switchover. There are no known workarounds.

Open Caveats for Release 12.2(15)BC2d

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)BC2d 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)BC2d.

Closed and Resolved Caveats for Release 12.2(15)BC2d

The caveats listed in Table 38 are resolved in Cisco IOS Release 12.2(15)BC2d. 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)BC2d

Caveat ID Number	Description

CSCef44517	Immediately after booting up, a PRE-1 may unexpectedly reload with the following error:
	`%ERR-1-GT64120 (PCI-1): Fatal error, PCI retry counter expired`
	`GT=0xB4000000,`
	`cause=0x00001000,`
	`mask=0x00D01D00, real_cause=0x00001000`
	`bus_err_high=0x00000000,`
	`bus_err_low=0x00000000,`
	`addr_decode_err=0x00000470`
	The fault is limited to PRE-1 version 08 with Texas Instrument PCI bridge chips. This version can be identified by the Top Assy. Part Number visually (on the box) or in the show chassis CLI command:
	`Top Assy. Part Number : 800-17437-08`
	`^^^`
	Workaround: Upgrade IOS to 12.2(15)BC1e or higher.
	Alternative workaround: Upgrade IOS to 12.2(15)BC2d or higher.

Open Caveats for Release 12.2(15)BC2c

All the caveats listed in Table 37 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 18 Open Caveats for Cisco IOS Release 12.2(15)BC2c

Caveat ID Number	Description
CSCdw08393	If you configure the **crypto key generate rsa** command on a Cisco 10000 series edge services router with dual performance routing engines (PREs), the command fails to synchronize to the secondary PRE. There are no known workarounds.
CSCea68692	If you configure the **crypto key generate rsa** command on a Cisco uBR10012 router with dual performance routing engines (PREs), the command fails to synchronize to the secondary PRE. Duplicate of CSCdw08393. This issue occurs when the crypto key generates rsa with dual PRE on uBR10012 router. Workaround: Reset the secondary PRE will generally work-around this failure.
CSCeb25866	Under certain conditions, the number of service flows on an interface, as reported by “show cable load-balance load”, does not match the real number of service flows. There are no known workarounds.
CSCeb71709	The uBR can only support 1 root certificate, which means only which ever certificate is loaded (North American) or European, BPI+ can only be enabled for those cards on which that type of certificate is loaded. There are no known workarounds.

Table 18 Open Caveats for Cisco IOS Release 12.2(15)BC2c (continued)

Caveat ID Number	Description

CSCeb76832	The Ubr1000k may keep reloading the Cable Linecards after a system reload. PRE will give the following errors forever:
	`01:34:08: %IPCOIR-3-LOADER_IPC_FAIL: IPC failed (timeout) sending download start message to slot 6/\ 1`
	`01:47:27: %IPCOIR-5-CARD_DETECTED: Card type 2cable-mc28c (0x235) in slot 6/1`
	`01:47:27: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/1`
	CLC will give the following errors forever:
	`%IPC-5-NULL: Recd. msg Dest Port=0x4, seq = 3`
	In addition, the legacy linecards (2x8, 1x6..) could give the following errors:
	`%IPCGRP-6-NOKEEP: Too long since a keepalive was received from the PRE.`
	`%IPCGRP-6-NOINBND: Unable to create "bpfe inbound register" port, error 7.`
	`...`
	`LOT 7/1: *Apr 18 06:30:31.075: %IPCGRP-6-NOTBHLPR: The PRE wants to download a card image, but we're not a boothelper.`
	Powercycling or reload of the entire box will recover this situation.
	There are no known workarounds.

CSCec04915	Intermittent ping failure is seen on the GE. There are no known workarounds.
CSCec35079	Under certain load conditions, modems may be stuck in init(rc) or other pre-registration states. This can occur if upstream service flows have a high priority and a guaranteed minimum bandwidth, and if the upstream capacity is completely consumed by traffic associated with such service flows. In this condition, new modems trying to come online may not receive any bandwidth grants, and may thus be stuck forever in init(rc) or other pre-initialization states until the traffic is reduced. With some modem types, it is also observed that affected modems start to request bandwidth with SID 0. Note that this condition _only_ occurs if, with above mentioned conditions, the upstream utilization is _constantly_ at its capacity, i.e., well above 90%. The upstream utilization can be checked with the following command where <interface> is the cable interface and <n> is the upstream channel: **show interface <interface> mac-scheduler <n>** The output of this command will include the following line: `Avg upstream channel utilization : xx%` The issues described in this ddts entry will only be seen if “xx” is constantly above 90% (and if upstream flows have a guaranteed minimum bandwidth). There are no known workarounds.

Table 18 Open Caveats for Cisco IOS Release 12.2(15)BC2c (continued)

Caveat ID Number	Description
CSCed07010	If before the PRE switchover, the protect interface was in Shut state and we do a no-shut after the PRE switchover, the protect interface may stay stuck in NON_FUNCTIONAL state. Workaround: Do a hw-module reset of the protect interface.
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.
CSCed74036	Enterprise routers behind cable modems may lose connectivity to the uBR10012 router. This issue is seen in 12.2(15)BC2. It may be in 12.2(15)BC1, but is not in 12.2(11)BC2. Workaround: Power cycle the cable modem (which may not be acceptable).
CSCed75425	Clearing counters on a uBR10012 router can cause SRP interface rate counters to be incorrectly reset to 0. There are no known workarounds.
CSCed85561	On a uBR10012 router with an MQC output service policy that sets precedence, the packets are correctly marked but the "show policy int [interface]" reports the "Packets marked" counter as 0 (zero). There are no known workarounds.
CSCed86151	All CMs on an US go down sporadically. **show cable modem summary total** reports for this specific US 0 modems registered, all modems are in offline. **show controllers cable** reports that *UCD Count* counter is still increasing. **show interfaces cable** reports that *Init Mtn Slots* and *Stn Mtn Slots* are also increasing. Workaround: Change the US frequency (manually). CMs come online and stay online even when the US frequency is changed back to the original one.
CSCed89210	When there is heavy traffic on the backhaul interface and the uBR10012 router is reloaded, then it is possible that the PXF gets reloaded 20 seconds after bootup, with an error message "C10KEVENTMGR-1-MINOR_FAULT: PXF DMA New Work Queue High Error". Workaround: Ensure that the traffic coming to the router is not very heavy immediately after bootup.
CSCed89265	OIR of GigE card can cause tail drops on other backhaul linecards in uBR10012 router. There are no known workarounds.
CSCee00895	In the uBR10012 router, packets switched by PXF are counted as process switched packets for the backhaul interfaces. These erroneous counts are displayed in "show interface switching" output. There are no known workarounds.

Table 18 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.
CSCee02399	After several line card switchovers in the presence of active packetcable calls, the active service flow count may go down on the CMTS. It has been observed that the CMTS deletes the service flow because it receives a DSD from the MTA/CM. It is possible that after several switchovers the MTA/CM gets into some state where it prematurely sends a DSD (before the call terminates). The reason as to why the MTA/CM sends a premature DSD is unknown. There are no known workarounds.
CSCee15560	After running voice calls for a while and conducting back to back LC swithcovers, it is observed that MTA may get into a state where they are considered down or may have lost NCS stack. Once in this mode, reset/power-cycle on MTA is needed to get them back in the state to make calls. It is mostly seen on Toshiba MTAs. There are no known workarounds.
CSCee32618	The CMTS may report the following error and trace back. `%GENERAL-3-EREVENT: No current_if_info` There are no known workarounds.
CSCee39660	The CMTS may report a traceback error during a PRE switch over. There are no known workarounds.
CSCee41060	Upstream Timing offsets not synced over to Protect linecard causing modem time alignments and drop packets. Workaround: Wait for a new modem to come online or a modem to flap, or shut/no shut the affected upstream port(s). Another work-around is to configure a high safety value in the dynamic map advance CLI command.
CSCee60254	The ifHCInOctets (.1.3.6.1.2.1.31.1.1.1.6) counters are very high for the gigabit interfaces on the UBR10000. 12.2(15)BC2 is the current IOS version on the UBR. There are no known workarounds.
CSCee62626	For systems with 25K or modem modems, the RP will become sluggish and the modem registration will become extremely slow. Workaround: Shut down bundle slaves or other LCs until approximately 75% of the modems on the non shut cards have registered. Then no shut the shut down cards.

Table 18 Open Caveats for Cisco IOS Release 12.2(15)BC2c (continued)

Caveat ID Number	Description

CSCee64987	The **Cable Arp Filter** commands are not removed from the Protect line after a revert. This has no operational impact on the CMTS.
	Workarounds: If the Protect card is no longer used in an hccp configuration, manually remove the following commands that would have been inappropriately been left on the Protect's configuration:
	`no cable arp filter reply`
	`no cable arp filter request`

CSCee93770	When modems simultaneously go offline on multiple line cards, the N+1 protocol may get into an inconsistent state. Modems cannot come online and the system does not recover. Some interfaces remain in an Updown Down state and modems can never come back online. Workaround: Hardware Module reset the Protect line card.
CSCee94943	SID not provided when running command **sh hard pxf cable source-verify**. This was seen internally while testing modem reset. The modem needs to be assign to a subinterface via DHCP. There are no known workarounds.
CSCef04085	After a N+1 switch over, traffic modem counters are not updated while the modem is active on the Protect line card. There are no known workarounds.
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.
CSCef14781	The PRE may report the error below during a PRE switchover. `%UBR10K-3-QUEUEFULL: Unable to enqueue since the queue is full` There are no known workarounds.
CSCef23937	N+1 switchovers will NOT work properly in a setup which does NOT have RF switch between the Working and Protect LC. Workaround: Have a dummy config line in the HCCP config for RF switch even if there is no RF switch physically present.
CSCef24484	Cable modem are associated to wrong sub-interface in a MPLS VPN setup This issue occurs when 2 DHCP server are defined/reacheable from each sub-interfaces networks. Workaround: Clear cable modem xxxx.xxxxx.xxxx del.

Closed and Resolved Caveats for Release 12.2(15)BC2c

The caveats listed in Table 38 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 19 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.
CSCec48483	Upon reloading both the Active and Standby PREs, after the system comes up, the protect line card comes up fine. But the working line card is in down down state. This is a rare condition that is not easily reproducible. Workaround: hw_module reset the working line card.
CSCed23795	During reload of a uBR10012 router, a traceback is seen. There are no known workarounds.

Table 19 Closed and Resolved Caveats for Release 12.2(15)BC2c (continued)

Caveat ID Number	Description

CSCed71560	uBR10012 router running 15BC1b fails dhcp for CPE inside a Motorola DCT5000 when no bundle entry is found for an incoming dhcp packet.
	This issue is restricted to only such settop boxes. Modems always come online ok on the same uBR10012 router and cable line card.
	Workaround: Follow the following steps:
	1. Feed the failing DCT CPE mac addr to the following CLI:
	`sh ip arp vrf internet <CPE mac addr>`
	The CLI output will give you the cable interface(s) that has to be cleaned up for offending IP addr entries in the CMTS bundling table.
	2. To find out offending IP entries in the CMTS bundle table, use the CMTS hidden CLI of:
	`sh int cx/y/z buck rp`
	Any "host" entry in the output that has the IP field "unavailable" is an offending entry. This entry has to be removed from the CMTS by invoking:
	`clear cable host <offending IP's mac addr>`
	3. Once all offending CMTS bundle entries are removed, reload the modem in the DCT5000 and now both modem and CPE will show up as registered on the CMTS.

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.

CSCee01627	In 12.2(15)BC2a and 12.2(15)BC2b, on a uBR10012 router, for bursty traffic, packets can be erroneously marked as non-conforming even when the average data rate is below the configured max rate. There are no known workarounds.

Table 19 Closed and Resolved Caveats for Release 12.2(15)BC2c (continued)

Caveat ID Number	Description
CSCee15965	Executing **show srp topology** for a uBR10012 router OC-12 SRP linecard gives false "Last received topology pkt" and "Last topology change was" values. This issue occurs if the OC-12 SRP card is on the ring, the interface is up, and the linecard is transmitting topology packets. There are no known workarounds.
CSCee20385	Under some congestion/traffic conditions, routing updates such as ISIS may get dropped. There are no known workarounds other than to investigate and throttle the traffic conditions causing the congestion.
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.
CSCee31581	Configuring hccp on the interface immediately after taking the interface out of shutdown causes the working interface to be stuck down. Workaround: Delay configuring hccp until the interface is up or configure hccp before taking the interface out of shutdown.
CSCee32609	The CMTS may report a CPU hog error when processing GetBulk SNMP requests. There are no known workarounds.
CSCee32628	The CMTS may report the following error: `%UBR10000-3-NOMEM: Failed to get buffer from flap-list private pool.` There are no known workarounds.
CSCee35423	PRE may unexpectedly reload if an interface is shut down and then HCCP is immediately unconfigured. There are no known workarounds.
CSCee62732	Call cannot be made if DS slack term exceeded. Workaround: Change the DS slack term in Call agent to 0. If one is using the Cisco BTS 3.5.X version, one can use the following command to change the slack term in their EMS system: `change ca-config type=DQOS-DS-SLACK-TERM; value=0` However, it's noticed in customer site, that this affects voice quality where choppy voice is heard, and impact service to customer.

Table 19 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.
CSCee64969	With BPI+ and secondary serv-flows, the standby line card (Protect or Working) will experience a memory leak when it is standby. The issue only occurs when BPI and secondary flows are in use. Workaround: Increase TEK key expire time from default of 12 hours to 18 or 24 hours. Alternative workaround: Reload the Protect line-card on memory depletion. With 512 MB of RAM on linecard, this should happen after ~2 months of operation.
CSCee65665	The CMTS may display the following error during an N+1 switch over: `GENERAL-3-EREVENT: No current_if_info` There are no known workarounds.
CSCee66747	HCCP may get into an inconsistent state (Protect doesn't load the Working's config completely) if back-to-back switchovers (Protect to Working1 and Working2 to Protect) are performed very quickly (via a cut n paste). There are no known workarounds.
CSCee67718	High volumes of incoming ARP traffic can cause routing adjacencies to flap on the uBR10012 router. Workaround: Throttle the ARP at the source.
CSCee69951	The src-verify lease-query filtering functionality may have the following issues: – Can configure threshold for downstream filter to greater than 255, even though it is not supported – Counter does not increment with filter threshold is set to 0. – Clear counters does not clear the filter counters There are no known workarounds.
CSCee71684	In certain cases, a classifier entry will not work after a switchover. There are no known workarounds.
CSCee76039	With 12.2(15)BC2d images, encrypted multicast will not work. Workaround: Do not encrypt multicast traffic.
CSCee78261	When CMTS is configured with spectrum group, issue the **no cable spectrum-group** command introducing some memory leaks. Moreover, the USs in the removed spectrum group have some bogus freq reassigned with 12.3BC image. There are no known workarounds.

Table 19 Closed and Resolved Caveats for Release 12.2(15)BC2c (continued)

Caveat ID Number	Description
CSCee79105	When ubr10k-k8p6-mz.122-15.BC2b is load on a 10k with SNMP polls from MRTG and What'sUp Gold and cpu utilization was < 35%. After loading the same image on the 2nd PRE and switching from secondary PRE to primary PRE, cpu utilization is now 100%. As a result console response is very slow. In addition to MRTG and What'sUp Gold, via getmany was also being poll. There are no known workarounds.
CSCee84392	In a MPLS/VPN environment, a cable modem using DOCSIS 1.0 becomes unreachable. The CPE attached to it is still reachable. This issue has been detected while resetting the modem. The sub-interface where the MOdem is assign to is configure with "cable source-verify dhcp" and "no cable arp". Workaround: Make sure "no cable arp" is unconfigured from the sub-interface default is "cable arp".
CSCee88307	This ddts is created to release the microcode for CSCee67718 and CSCee20385 that are being fixed in the 12.2(15)BC2c ERS release. There are no known workarounds.
CSCef04522	When a uBR10012 router boots up, the internal packet memory in the switching path for one or more linecards can get stuck due to an initialization error on the linecard. When the **exception pxf ipm** command is enabled, this IPM stuck state will be detected and result in a PXF reload. While reloading PXF, the RP can crash. There are no known workarounds.
CSCef04614	Improve cable modem bring up performance on a uBR10012 router. There are no known workarounds.
CSCef10097	With Dynamic UGS serv-flows based Voice Calls, on LC switchover, the uBR10K-LC may reload unexpectedly. The specifics of this issue are as follows: BPI+ is on, a voice call (dynamic serv-flow) gets established and then gets destroyed. An LC switchover here may unexpectedly reload the LC. This issue does not occur when all voice calls stay active. There are no known workarounds.,
CSCef13047	DOCSIS 1.0+ on uBR10012 router running 12.2(15)BC2b drops downstream voice packets resulting in one-way voice. There are no known workarounds.
CSCin54055	DOCSIS1.0 Qos profile created by CM is not seen in "show cable qos profile" CLI output after PRE switchover. There are no known workarounds.

Table 19 Closed and Resolved Caveats for Release 12.2(15)BC2c (continued)

Caveat ID Number	Description
CSCin75900	The networks connected to the CPE router (in case of business customers) become unreachable after PRE switchover if "cable source-verify [dhcp]" is configured on the CMTS (sub)interface associated with the modem. There are no known workarounds.
CSCin76192	Traceback can be observed in an image with a fix for CSCee32628 during flap list aging. There are no known workarounds.

Open Caveats for Release 12.2(15)BC2b

All the caveats listed in Table 37 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 20 Open Caveats for Cisco IOS Release 12.2(15)BC2b

Caveat ID Number	Description
CSCea68692	If you configure the **crypto key generate rsa** command on a Cisco uBR10012 router with dual performance routing engines (PREs), the command fails to synchronize to the secondary PRE. Duplicate of CSCdw08393. This issue occurs when the crypto key generate rsa with dual PRE on uBR10012 router. Workaround: Reset the secondary PRE will generally work around this failure.
CSCeb25866	Under certain conditions, the number of service flows on an interface, as reported by "show cable load-balance load", does not match the real number of service flows. There are no known workarounds.
CSCeb71709	The uBR can only support 1 root certificate, which means only which ever certificate is loaded (North American) or European, BPI+ can only be enabled for those cards on which that type of certificate is loaded. There are no known workarounds.

Table 20 Open Caveats for Cisco IOS Release 12.2(15)BC2b (continued)

Caveat ID Number	Description

CSCeb76832	The Ubr1000k may keep reloading the Cable Linecards after a system reload.
	PRE will give the following errors forever:
	`01:34:08: %IPCOIR-3-LOADER_IPC_FAIL: IPC failed (timeout) sending download start message to slot 6/\ 1`
	`01:47:27: %IPCOIR-5-CARD_DETECTED: Card type 2cable-mc28c (0x235) in slot 6/1`
	`01:47:27: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/1`
	CLC will give the following errors forever:
	`%IPC-5-NULL: Recd. msg Dest Port=0x4, seq = 3`
	In addition, the legacy linecards (2x8, 1x6..) could give the following errors:
	`%IPCGRP-6-NOKEEP: Too long since a keepalive was received from the PRE.`
	`%IPCGRP-6-NOINBND: Unable to create "bpfe inbound register" port, error 7.`
	`...`
	`LOT 7/1: *Apr 18 06:30:31.075: %IPCGRP-6-NOTBHLPR:The PRE wants to download a card image, but we're not a boothelper.`
	Powercycling or reload of the entire box will recover this situation.
	There are no known workarounds.

CSCec04915	Intermittent ping failure is seen on the GE. There are no known workarounds.
CSCec35079	Under certain load conditions, modems may be stuck in init(rc) or other pre-registration states. This can occur if upstream service flows have a high priority and a guaranteed minimum bandwidth, and if the upstream capacity is completely consumed by traffic associated with such service flows. In this condition, new modems trying to come online may not receive any bandwidth grants, and may thus be stuck forever in init(rc) or other pre-initialization states until the traffic is reduced. With some modem types, it is also observed that affected modems start to request bandwidth with SID 0. Note that this condition _only_ occurs if, with above mentioned conditions, the upstream utilization is _constantly_ at its capacity, i.e., well above 90%. The upstream utilization can be checked with the following command: show interface <interface> mac-scheduler <n> where <interface> is the cable interface and <n> is the upstream channel. The output of this command will include the following line: Avg upstream channel utilization : xx% The problem described in this ddts entry will only be seen if “xx” is constantly above 90% (and if upstream flows have a guaranteed minimum bandwidth).

Table 20 Open Caveats for Cisco IOS Release 12.2(15)BC2b (continued)

Caveat ID Number	Description
CSCec48483	Upon reloading both the Active and Standby PREs, after the system comes up, the protect line card comes up fine. But the working line card is in down down state. This is a rare condition that is not easily reproducible. Workaround: hw_module reset the working line card.
CSCed07010	If before the PRE switchover, the protect interface was in Shut state and we do a no-shut after the PRE switchover, the protect interface may stay stuck in NON_FUNCTIONAL state. Workaround: Do a hw-module reset of the protect interface.
CSCed74036	Enterprise routers behind cable modems may lose connectivity to the uBR10012 router. This symptom is seen in 12.2(15)BC2. It may be in 12.2(15)BC1, but is not in 12.2(11)BC2. Workaround: Power cycle the cable modem (which may not be acceptable).
CSCed75425	Clearing counters on a uBR10012 router can cause SRP interface rate counters to be incorrectly reset to 0. There are no known workarounds.
CSCed85561	On a uBR10012 router with an MQC output service policy that sets precedence, the packets are correctly marked but the “show policy int [interface]” reports the “Packets marked” counter as 0 (zero). There are no known workarounds.
CSCed86151	All CMs on an US go down sporadically. The command **show cable modem summary total** reports for this specific US 0 modems registered, all modems are in offline. The command **show controllers cable** reports that *UCD Count* counter is still increasing. The command **show interfaces cable** reports that *Init Mtn Slots* and *Stn Mtn Slots* are also increasing. Workaround: Change the US frequency (manually). CMs come online and stay online even when the US frequency is changed back to the original one.
CSCed89210	When there is heavy traffic on the backhaul interface and the uBR10012 router is reloaded, then it is possible that the PXF gets reloaded 20 seconds after bootup, with an error message 'C10KEVENTMGR-1-MINOR_FAULT: PXF DMA New Work Queue High Error' Workaround: Ensure that the traffic coming to the router is not very heavy immediately after bootup.
CSCed89265	OIR of OC-48 POS card can cause tail drops on other backhaul linecards in uBR10012 router. There are no known workarounds.
CSCee00895	In the uBR10012 router, packets switched by PXF are counted as process switched packets for the backhaul interfaces. These erroneous counts are displayed in “show interface switching” output.

Table 20 Open Caveats for Cisco IOS Release 12.2(15)BC2b (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.
CSCin54055	DOCSIS1.0 Qos profile created by CM is not seen in "show cable qos profile" CLI output after PRE switchover. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC2b

The caveats listed in Table 38 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 21 Closed and Resolved Caveats for Release 12.2(15)BC2b

Caveat ID Number	Description
CSCec75766	GigE firmware image download may fail when multiple GigE cards are installed in uBR10012 router chassis. There are no known workarounds.
CSCed29019	Ported a fix to handle auto negotiation between a c10k gigE port and a cat 4k gigE port. A 15 msec delay is needed to allow autonegotiation between these 2 interfaces. There are no known workarounds.
CSCed46270	In rare circumstances, the traceback described in this DDTS may be seen on the RP console. This is caused due to a race condition in the previous HCCP switchover. Traffic to and from modems on the subinterface affected will be impacted. Workaround: Perform another HCCP (LC) switchover to clear the problem.

Table 21 Closed and Resolved Caveats for Release 12.2(15)BC2b (continued)

Caveat ID Number	Description
CSCed86358	A cable line card running IOS may crash. In some cases if the card does not have enough memory, it will crash to ROMMON and will not automatically reboot. This issue occurs under the following conditions: • HCCP must be configured on the linecard • Secondary service flows must be configured via the cable modem config file • A modem must have at one time been online and then gone offline and remain offline during an hccp switchover. The service flows for that modem are not de-allocated when it goes offline and are the source of the crash. • Performing a “show cable tech” or “show int CableX/Y/Z sid” after the switchover will access the sids that were not de-allocated and may crash either the card that has become Active or, if another switchover is done, the card that is Standby. There are no known workarounds other than to not configure secondary service flows if they are not truly needed.
CSCed91708	On MC520 cable line cards, the input packet rate and input bit rate, as shown in the 'show interface <interface>' command, can become very small when the input packet count is greater than 2^31, but has not yet wrapped back to 0. The input rates will return to correct values when the input packet count has wrapped through 0. There are no known workarounds.
CSCee01374	The PRE may crash when multiple simultaneous config sessions are executed via VTY and HCCP is configured in the cable interfaces. There are no known workarounds.
CSCee02150	After a CMTS is loaded, the “IP Input” process is consuming a few percentage points of the CPU as shown by “show proc cpu sort”. It is possible that worms on CPEs behind modems are scanning IP ports in the network. This will result in arp request packets being broadcast and passing through the arp filter. This change allows the operator to see on a per-modem basis which modems are the highest source of the traffic and thus which end users and modems to focus on for applying counter-measures such as ACLs. There are no known workarounds. This is a tweak to the new arp filter feature to show more IP-centric data.
CSCee08290	If modems are deleted/reset in bulk using clear cable modem all delete/reset command, it may cause a CPU-Hog message or may sometimes cause the cable line card to reset. There are no known workarounds.

Table 21 Closed and Resolved Caveats for Release 12.2(15)BC2b (continued)

Caveat ID Number	Description
CSCee16606	Cable intercept might not send copy of Downstream packets to the collection server, only Upstream packets might appear on the collection server. This problem is seen with IOS 12.2(15)BC1b image. Three ar e no known workarounds.
CSCee20584	Traffic to secondary addresses on a uBR10012 router such as telnet or ping traffic can be affected by other low priority traffic being diverted to the RP, if there is a lot of such traffic is being punted. Workaround: Use primary address for telnet and ping.
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 no known workarounds.
CSCee21114	When “source-verify dhcp” and “no cable arp” are 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”.
CSCee22333	Working line-cards may reload during a LC switch-over. The number of line-cards that fail is random. There are no known workarounds.
CSCee24107	The slot preference algorithm gives preference to PRE-A to become the active after a reload. This algorithm sometimes was not working, and PRE-B become the active on reload. Workaround: Do a PRE swtichover (redundancy force failover) if PRE-B became active.
CSCee25855	The Linecard that is becoming active could crash. There are no known workarounds.
CSCee27859	With VI configured, there is delay between switchover of interfaces on the same LC (CSCee40287). A CLI switchover command issued during this time window when one interface on the card is ready to switch while others are still not, could lead to traceback or linecard crash. There are no known workarounds.
CSCee35624	The Line Card may crash after a N+1 switchover. There are no known workarounds.

Table 21 Closed and Resolved Caveats for Release 12.2(15)BC2b (continued)

Caveat ID Number	Description
CSCee40287	With VI configured, all interfaces on the LC must switch simultaneously. However, it is possible to experience a several seconds delay between switchover of the interfaces on the same card. That leads to the situation where one interface on the LC is ready for switchover several seconds before other interfaces become ready. CLI switchovers issued during this delay can lead to instability. Workaround: Wait for all interfaces on the LC to be ready for switchover before issuing CLI switchover.
CSCee46449	Multicast packets punted when destination going out the POS interface. There are no known workarounds.
CSCee47418	If a line-card switch-over is performed with at least 3500 modems, 3us3ds service flows, 20-30% modems will go offline during the switch-over. Modems will re-range and come back online. There are no known workarounds.
CSCee52001	Under rare circumstances, an ASSERTION FAILED message followed by a crash may be seen on ubr10000, in or around line 416 of sch_rp_docsis11.c. This will be followed by endless ASSERTION FAILED messages in or around lines 430 and 437. If there is no console connection when the problem occurs, and the console connection is created later, the system may display random characters forever, and it will not respond to any external events. System must be hard reset (power cycled) to recover if there is no secondary PRE. This issue is seen in 12.2(15)BC1, 12.2(15)BC2, and possibly in all uBR10012 router SW images. This is more likely to occur with small arp timeout values. There are no known workarounds. However, tt is recommended not to change the ARP timeout from its default value.
CSCee57481	UBR10K-6-CM_INCONSISTENCY messages may be seen on the RP console after a LineCard failover. This condition is seen if modems on a particular upstream (or downstream) are forced offline and re-range on another upstream (or downstream). There are no known workarounds.
CSCee58844	High priority traffic punted to the RP on a uBR10012 router can get dropped due to a backup in the high priority punt queue. As a result, SNMP monitoring, pings and routing update traffic can get dropped. Workaround: Make changes to the configuration in the network to reduce high priority punted traffic. e.g. If the priority queue is backing up due to ARP, enabling ARP filters and configuring 'no cable arp' can help.

Table 21 Closed and Resolved Caveats for Release 12.2(15)BC2b (continued)

Caveat ID Number	Description
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.
CSCin71861	If 255 CPE’s are configured behind CM's in the system, the primary PRE will crash. Workaround: Configure some small number of allowable CPE’s like 15 to 25.
CSCin74377	When CMTS is configured with the shared spectrum group using time scheduled bands and then removal of spectrum group definition may cause CMTS to crash. Spectrum management software module is modified to remove the spectrum group in the proper sequence. There are no known workarounds.

Open Caveats for Release 12.2(15)BC2a

All the caveats listed in Table 37 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 22 Open Caveats for Cisco IOS Release 12.2(15)BC2a

Caveat ID Number	Description
CSCdx78723	Both Working & protect interfaces may become active for a short period if the Working line card is reset or OIRed. There are no known workarounds.

CSCdz28737	When in the interface configuration mode:
	`conf t`
	`interface x/y`
	If the standby PRE is coming up and a configuration is entered on the primary PRE it will not be synched across to the secondary PRE.
	Workaround: Wait until the standby PRE is in Hot Standby before entering the interface configuration mode.
	Alternative workaround: Exit the interface configuration mode and re-enter. Then re-issue the configuration commands

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCea68692	If you configure the **crypto key generate rsa** command on a Cisco uBR10012 router with dual performance routing engines (PREs), the command fails to synchronize to the secondary PRE. Duplicate of CSCdw08393. This issue occurs when the crypto key generates rsa with dual PRE on uBR10012 router. Workaround: Reset the secondary PRE.
CSCea93194	Under rare situations the output rate counter could display an incorrect value. This cosmetic error shows up when doing the command: show interface Gx/y/z. There are no known workarounds.
CSCeb25866	Under certain conditions, the number of service flows on an interface, as reported by "show cable load-balance load", does not match the real number of service flows. There are no known workarounds.
CSCeb48408	In Cable/MPLS setup show cable modem sporadically shows cable modems with duplicate IP addresses, of which one cable modem has IP address which does not corresponds to one given by DHCP server and clearly shown in DHCP debugs. At the same time show arp shows correct entries. If tftp-enforce is used this can cause "problematic" cable modem to be blocked and shown not to trying tftp download, even if tftp server logs indicate opposite. Without tftp-enforce, cable modem with duplicate IP address is on-line and have full IP connectivity. Clear cable modem does not help. Workaround: reload CMTS.
CSCeb59134	The uBR10012 with MC520S occurs the load of CPU becomes 100% every one hour with "cable modem remote-query" by polling_process. This issue occurs under the following conditions: Platform: uBR10012 with MC520S IOS : ubr10k-k8p6-mz.122-11.BC3a Config : cable modem remote-query 3600 public Workaround: Use no cable modem remote-query.
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.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCeb63497	After a PRE switch over, a line card may not be operational and modems will fail to come online. A hw-module reset is required to make the card operational. There are no known workarounds.
CSCeb71709	The uBR can only support 1 root certificate, which means only which ever certificate is loaded (North American) or European, BPI+ can only be enabled for those cards on which that type of certificate is loaded. There are no known workarounds.

CSCeb76832	The Ubr1000k may keep reloading the Cable Linecards after a system reload.
	`PRE will give the following errors forever:`
	`01:34:08: %IPCOIR-3-LOADER_IPC_FAIL: IPC failed (timeout) sending download start message to slot 6/\`
	`1`
	`01:47:27: %IPCOIR-5-CARD_DETECTED: Card type 2cable-mc28c (0x235) in slot 6/1`
	`01:47:27: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/1`
	`CLC will give the following errors forever:`
	`%IPC-5-NULL: Recd. msg Dest Port=0x4, seq = 3`
	`In addition, the legacy linecards (2x8, 1x6..) could give the foll. errors;`
	`%IPCGRP-6-NOKEEP: Too long since a keepalive was received from the PRE.`
	`%IPCGRP-6-NOINBND: Unable to create "bpfe inbound register" port, error 7.`
	`...`
	`LOT 7/1: *Apr 18 06:30:31.075: %IPCGRP-6-NOTBHLPR: The PRE wants to download a card image, but we'r\`
	`e not a boothelper.`
	Powercycling or reload of the entire box will recover this situation.
	There are no known workarounds.

CSCec04915	Intermittent ping failure is seen on the GE. There are no known workarounds.
CSCec35079	Under certain load conditions, modems may be stuck in init(rc) or other pre-registration states. This can occur if upstream service flows have a high priority and a guaranteed minimum bandwidth, and if the upstream capacity is completely consumed by traffic associated with such service flows. In this condition, new modems trying to come online may not receive any bandwidth grants, and may thus be stuck forever in init(rc) or other pre-initialization states until the traffic is reduced. With some modem types, it is also observed that affected modems start to request bandwidth with SID 0. There are no known workarounds.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCec48483	Upon reloading both the Active and Standby PREs, after the system comes up, the protect line card comes up fine. But the working line card is in down down state. This is a rare condition that is not easily reproducible. Workaround: hw_module resets the working line card.
CSCed02523	Trying to block multicast on subinterface with: no cable ip-multicast-echo on some subinterfaces. This works when applied to the main interface but when applied to a subinterface, it does not block packets arriving from that interface. There are no known workarounds.
CSCed07010	If before the PRE switchover, the protect interface was in Shut state and we do a no-shut after the PRE switchover, the protect interface may stay stuck in NON_FUNCTIONAL state. Workaround: Do a hw-module reset of the protect interface.

CSCed23627	Under rare circumstances, the system may reboot with the following error message.
	`%SYS-1-MTNOTFENCED: Expired timer is not fenced, timer = 0, type 0`
	`%Software-forced reload`
	There are no known workarounds.

CSCed45792	The following error message may be seen on the uBR10012 router: `%UBR10000-5-MAXHOST: Interface <int>, New host with IP address a.b.c.d and MAC xxxx.xxxx.xxxx on SID yyyy (CM zzzz.zzzz.zzzz) is ignored.` This is a normal condition if the number of hosts exceeds the number of hosts permitted for a given cable modem. However, the output of "show cable modem zzzz.zzzz.zzzz verbose" may indicate that the permitted number of hosts has not been reached, which is unexpected. This condition occurs if there are hosts with unknown IP address in the system. To see those hosts, enter the command **show interface <int> modem <sid> rp** There are no known workarounds.
CSCed47913	At the first installation of MC5X20, CM client can not register successfully, after "shut" & "no shut" for several times, CM could register. But after running for some time, all CM could be dropped, and you should shut & "no shut" again to let CM register again. This issue occurs during first installation and running. Workaround: shut then no shut the cable interface.
CSCed51052	Cable source verify may drive the RP CPU to high values. Workaround: Disable cable source-verify (if acceptable).

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCed53717	C10K BPE IP Enqueue process consumes high CPU in steady state. There are no known workarounds.
CSCed54247	It has been observed that sometimes after fixing upstream RF outage, original number of cable modems don't come back online, only a fraction (like 25%) comes online. Changing the upstream frequency to different frequency bring cable modems online. Once all the cable modems are online, customer again change the upstream frequency to back to original one. This issue is reported by customer on upstreams with 700+ cable modems on uBR10012 router and uBR7246VXR router. There are no known workarounds.
CSCed71560	uBR10012 router running 15BC1b reports wrong DHCP option 82 values intermittently. There are no known workarounds.
CSCed74036	Enterprise routers behind cable modems may lose connectivity to the uBR10012 router. This symptom is seen in 12.2(15)BC2. It may be in 12.2(15)BC1, but is not in 12.2(11)BC2. Workaround: Power cycle the cable modem (which may not be acceptable).
CSCed75425	Clearing counters on a uBR10012 router can cause SRP interface rate counters to be incorrectly reset to 0. There are no known workarounds.
CSCed79155	The 'show cable modem <ip address>' may not show any information for an offline modem. Workaround: show cable modem | include ip address.
CSCed85561	On a uBR10012 router with an MQC output service policy that sets precedence, the packets are correctly marked but the “show policy int [interface]” reports the “Packets marked” counter as 0 (zero). There are no known workarounds.
CSCed86151	All CMs on an US go down sporadically. **show cable modem summary total** reports for this specific US 0 modems registered, all modems are in offline. **show controllers cable** reports that *UCD Count* counter is still increasing. **show interfaces cable** reports that *Init Mtn Slots* and *Stn Mtn Slots* are also increasing. Workaround: Change the US frequency (manually). CMs come online and stay online even when the US frequency is changed back to the original one.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCed89210	When there is heavy traffic on the backhaul interface and the uBR10012 router is reloaded, then it is possible that the PXF gets reloaded 20 seconds after bootup, with an error message 'C10KEVENTMGR-1-MINOR_FAULT: PXF DMA New Work Queue High Error'. Workaround: Ensure that the traffic coming to the router is not very heavy immediately after bootup.
CSCed89265	OIR of OC-48 POS card can cause tail drops on other backhaul linecards in uBR10012 router. There are no known workarounds.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCed96245	On a uBR10012 router running 12.2(15)BC1b service flow's may not match the qos profile. The service flow has the same us/ds bandwith parameters as the modem config file but the qos displayed does not match. This may affect all modems or qos profiles. ex. ubr10000#show cable qos profile ID Prio Max Guarantee Max Max TOS TOS Create B IP prec. upstream upstream downstream tx mask value by priv rate bandwidth bandwidth bandwidth burst enab enab 1 0 0 0 0 0 0x0 0x0 cmts(r) no no 2 0 64000 0 1000000 0 0x0 0x0 cmts(r) no no 3 7 31200 31200 0 0 0x0 0x0 cmts yes no 4 7 87200 87200 0 0 0x0 0x0 cmts yes no 5 1 350000 0 3100000 0 0x0 0x0 cm no no 6 1 64000 0 128000 0 0x0 0x0 cm no no 7 1 640000 0 4000000 0 0x0 0x0 cm no no 8 1 180000 0 3100000 0 0x0 0x0 cm no no ubr10000#sh cable modem 0000.0000.0001 registered Interface Prim Online Timing Rec QoS CPE IP address MAC address Sid State Offset Power C5/1/2/U4 44 online 1318 0.00 6 1 10.0.0.1 0000.0000.0001 ubr10000#show cable qos profile 6 ID Prio Max Guarantee Max Max TOS TOS Create B IP prec. upstream upstream downstream tx mask value by priv rate bandwidth bandwidth bandwidth burst enab enab 6 1 64000 0 128000 0 0x0 0x0 cm no no The behavior was discover on a uBR10012 router running IOS 12.2(15)BC1b. The value seems to be incorrect only for the command <show cable profile (x)>. SNMP will verify correct paramters are being used: docsIfQosProfMaxUpBandwidth.1 docsIfQosProfMaxDownBandwidth.1 Workaround: Presently there is no workaround for this issue other then using SNMP.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCed96250	UGS voice packets on a uBR10012 router may be delayed. This causes choppy voice in the US. There are no known workarounds.
CSCee00895	In the uBR10012 router, packets switched by PXF are counted as process switched packets for the backhaul interfaces. These erroneous counts are displayed in 'show interface switching' output. There are no known workarounds.
CSCee01374	The PRE may crash when multiple simultaneous config sessions are executed via VTY and HCCP is configured in the cable interfaces. There are no known workarounds.
CSCee01703	RP may crash with the use of particular config file. 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.
CSCee06180	On the uBR10012 router, cable line card 5x20S may get broken. At that instance all the communication between 5x20 line card and main processor is stopped and card disappeared from all show commands. The following message displayed in cmts console log `.... %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot x/y` Workaround: To recover cable line card, issue the following command **CMTS# hw-module slot x reset** Where x and y are slot and subslot numbers
CSCee09412	If LC switch over happen before PRE switch over and there is some CM in online(d) state, after PRE switch over, these CM online(d) are not in RP database and cannot be seen from PR. For example ping cannot be successful and SNMP poll cdxCmCpeEntry will fail. Workaround: Reset those CM online(d) by cli “clear cable modem <xxx> reset”.
CSCee12121	LED of DS ports at mc520s-d light up after reloading uBR10012 router. However, **showdown** command was configured the DS ports. Workaround: Configre **no shutdown**, then LED is lights-out.
CSCin54055	DOCSIS1.0 Qos profile created by CM is not seen in “show cable qos profile” CLI output after PRE switchover. There are no known workarounds.

Table 22 Open Caveats for Cisco IOS Release 12.2(15)BC2a (continued)

Caveat ID Number	Description
CSCin56782	CMTS may crash when protector interface made shutdown and the HCCP configurations removal from the working interfaces. There are no known workarounds.
CSCin59835	CMTS may experience spurious memory access with RPR+ switch over. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC2a

The caveats listed in Table 38 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 23 Closed and Resolved Caveats for Release 12.2(15)BC2a

Caveat ID Number	Description
CSCee08163	The PRE may hang during an N+1 line card switchover with “cable source verify dhcp” enabled. It is caused due to a race condition in the code. There are no known workarounds.
CSCee13327	The output of “show pxf cable source-verify | i <sid>” will show different Fib Index for CM and CPE or multiple entries for the same IP address and SID but different Fib index. Workaround: Do not configure “cable source-verify [dhcp]”.
CSCee14029	Excessive source verify punts to the RP on the uBR10012 router can render the router unusable temporarily. Workaround: Unconfigure source-verify.

Open Caveats for Release 12.2(15)BC2

All the caveats listed in Table 37 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 24 Open Caveats for Cisco IOS Release 12.2(15)BC2

Caveat ID Number	Description
CSCdx78723	Both Working & protect interfaces may become active for a short period if the Working line card is reset or OIRed. There are no known workarounds.

CSCdz28737	When in the interface configuration mode:
	`conf t`
	`interface x/y`
	If the standby PRE is coming up and a configuration is entered on the primary PRE it will not be synched across to the secondary PRE.
	Workaround: Wait until the standby PRE is in Hot Standby before entering the interface configuration mode.
	Alternative workaround: Exit the interface configuration mode and re-enter. Then re-issue the configuration commands

CSCea68692	If you configure the **crypto key generate rsa** command on a Cisco uBR10012 router with dual performance routing engines (PREs), the command fails to synchronize to the secondary PRE. Duplicate of CSCdw08393. This issue occurs when the crypto key generates rsa with dual PRE on the uBR10012 router. Workaround: Reset the secondary PRE.
CSCea93194	Under rare situations the output rate counter could display an incorrect value. This cosmetic error shows up when doing the command: show interface Gx/y/z. There are no known workarounds.
CSCeb25866	Under certain conditions, the number of service flows on an interface, as reported by “show cable load-balance load”, does not match the real number of service flows. There are no known workarounds.

Table 24 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCeb48408	In Cable/MPLS setup show cable modem sporadically shows cable modems with duplicate IP addresses, of which one cable modem has IP address which does not corresponds to one given by DHCP server and clearly shown in DHCP debugs. At the same time show arp shows correct entries. If tftp-enforce is used this can cause "problematic" cable modem to be blocked and shown not to trying tftp download, even if tftp server logs indicate opposite. Without tftp-enforce, cable modem with duplicate IP address is on-line and have full IP connectivity. Clear cable modem does not help. Workaround: reload CMTS.
CSCeb59134	The uBR10012 with MC520S occurs the load of CPU becomes 100% every one hour with "cable modem remote-query" by polling_process. This issue occurs under the following conditions: Platform: uBR10012 with MC520S IOS : ubr10k-k8p6-mz.122-11.BC3a Config : cable modem remote-query 3600 public Workaround: Use no cable modem remote-query.
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.
CSCeb63497	After a PRE switch over, a line card may not be operational and modems will fail to come online. A hw-module reset is required to make the card operational. There are no known workarounds.
CSCeb71709	The uBR can only support 1 root certificate, which means only which ever certificate is loaded (North American) or European, BPI+ can only be enabled for those cards on which that type of certificate is loaded. There are no known workarounds.

Table 24 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCeb76832	The Ubr1000k may keep reloading the Cable Linecards after a system reload. PRE will give the following errors forever: 01:34:08: %IPCOIR-3-LOADER_IPC_FAIL: IPC failed (timeout) sending download start message to slot 6/\ 1 01:47:27: %IPCOIR-5-CARD_DETECTED: Card type 2cable-mc28c (0x235) in slot 6/1 01:47:27: %IPCOIR-5-CARD_LOADING: Loading card in slot 6/1 CLC will give the following errors forever: %IPC-5-NULL: Recd. msg Dest Port=0x4, seq = 3 In addition, the legacy linecards (2x8, 1x6..) could give the foll. errors; %IPCGRP-6-NOKEEP: Too long since a keepalive was received from the PRE. %IPCGRP-6-NOINBND: Unable to create "bpfe inbound register" port, error 7. ... LOT 7/1: *Apr 18 06:30:31.075: %IPCGRP-6-NOTBHLPR: The PRE wants to download a card image, but we'r\ e not a boothelper. Powercycling or reload of the entire box will recover this situation. There are no known workarounds.
CSCec04915	Intermittent ping failure is seen on the GE. There are no known workarounds.
CSCec35079	Under certain load conditions, modems may be stuck in init(rc) or other pre-registration states. This can occur if upstream service flows have a high priority and a guaranteed minimum bandwidth, and if the upstream capacity is completely consumed by traffic associated with such service flows. In this condition, new modems trying to come online may not receive any bandwidth grants, and may thus be stuck forever in init(rc) or other pre-initialization states until the traffic is reduced. With some modem types, it is also observed that affected modems start to request bandwidth with SID 0. There are no known workarounds.
CSCec48483	Upon reloading both the Active and Standby PREs, after the system comes up, the protect line card comes up fine. But the working line card is in down down state. This is a rare condition that is not easily reproducible. Workaround: hw_module resets the working line card.

Table 24 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed02523	Trying to block multicast on subinterface with: no cable ip-multicast-echo on some subinterfaces. This works when applied to the main interface but when applied to a subinterface, it does not block packets arriving from that interface. There are no known workarounds.
CSCed07010	If before the PRE switchover, the protect interface was in Shut state and we do a no-shut after the PRE switchover, the protect interface may stay stuck in NON_FUNCTIONAL state. Workaround: Do a hw-module reset of the protect interface.

CSCed23627	Under rare circumstances, the system may reboot with the following error message.
	`%SYS-1-MTNOTFENCED: Expired timer is not fenced, timer = 0, type 0`
	`%Software-forced reload`
	There are no known workarounds.

CSCed45792	The following error message may be seen on ubr10k: `%UBR10000-5-MAXHOST: Interface <int>, New host with IP address a.b.c.d and MAC xxxx.xxxx.xxxx on SID yyyy (CM zzzz.zzzz.zzzz) is ignored.` This is a normal condition if the number of hosts exceeds the number of hosts permitted for a given cable modem. However, the output of "show cable modem zzzz.zzzz.zzzz verbose" may indicate that the permitted number of hosts has not been reached, which is unexpected. This condition occurs if there are hosts with unknown IP address in the system. To see those hosts, enter the command **show interface <int> modem <sid> rp** There are no known workarounds.
CSCed47913	At the first installation of MC5X20, CM client can not register successfully, after "shut" & "no shut" for several times, CM could register. But after running for some time, all CM could be dropped, and you should shut & "no shut" again to let CM register again. This issue occurs during first installation and running. Workaround: shut then no shut the cable interface.
CSCed51052	Cable source verify may drive the RP CPU to high values. Workaround: Disable cable source-verify (if acceptable).
CSCed53717	C10K BPE IP Enqueue process consumes high CPU in steady state. There are no known workarounds.

Table 24 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed54247	It has been observed that sometimes after fixing upstream RF outage, original number of cable modems don't come back online, only a fraction (like 25%) comes online. Changing the upstream frequency to different frequency bring cable modems online. Once all the cable modems are online, customer again change the upstream frequency to back to original one. This issue is reported by customer on upstreams with 700+ cable modems on ubr10k and onubr7200VXR There are no known workarounds.
CSCed71560	UBR10K running 15BC1b reports wrong DHCP option 82 values intermittently. There are no known workarounds.
CSCed74036	Enterprise routers behind cable modems may lose connectivity to the ubr10k. This symptom is seen in 12.2(15)BC2. It may be in 12.2(15)BC1, but is not in 12.2(11)BC2. Workaround: Power cycle the cable modem (which may not be acceptable).
CSCed75425	Clearing counters on a uBR10k can cause SRP interface rate counters to be incorrectly reset to 0. There are no known workarounds.
CSCed79155	The 'show cable modem <ip address>' may not show any information for an offline modem. Workaround: show cable modem | include ip address.
CSCed85561	On a ubr10k with an MQC output service policy that sets precedence, the packets are correctly marked but the “show policy int [interface]” reports the “Packets marked” counter as 0 (zero). There are no known workarounds.
CSCed86151	All CMs on an US go down sporadically. **show cable modem summary total** reports for this specific US 0 modems registered, all modems are in offline. **show controllers cable** reports that *UCD Count* counter is still increasing. **show interfaces cable** reports that *Init Mtn Slots* and *Stn Mtn Slots* are also increasing. Workaround: Change the US frequency (manually). CMs come online and stay online even when the US frequency is changed back to the original one.
CSCed89210	When there is heavy traffic on the backhaul interface and the uBR10012 router is reloaded, then it is possible that the PXF gets reloaded 20 seconds after bootup, with an error message 'C10KEVENTMGR-1-MINOR_FAULT: PXF DMA New Work Queue High Error'. Workaround: Ensure that the traffic coming to the router is not very heavy immediately after bootup.

Table 24 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed89265	OIR of OC-48 POS card can cause tail drops on other backhaul linecards in uBR10k. There are no known workarounds.

Table 24 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed96245	On a uBR10012 router running 12.2(15)BC1b service flow's may not match the qos profile. The service flow has the same us/ds bandwith parameters as the modem config file but the qos displayed does not match. This may affect all modems or qos profiles. ex. ubr10000#show cable qos profile ID Prio Max Guarantee Max Max TOS TOS Create B IP prec. upstream upstream downstream tx mask value by priv rate bandwidth bandwidth bandwidth burst enab enab 1 0 0 0 0 0 0x0 0x0 cmts(r) no no 2 0 64000 0 1000000 0 0x0 0x0 cmts(r) no no 3 7 31200 31200 0 0 0x0 0x0 cmts yes no 4 7 87200 87200 0 0 0x0 0x0 cmts yes no 5 1 350000 0 3100000 0 0x0 0x0 cm no no 6 1 64000 0 128000 0 0x0 0x0 cm no no 7 1 640000 0 4000000 0 0x0 0x0 cm no no 8 1 180000 0 3100000 0 0x0 0x0 cm no no ubr10000#sh cable modem 0000.0000.0001 registered Interface Prim Online Timing Rec QoS CPE IP address MAC address Sid State Offset Power C5/1/2/U4 44 online 1318 0.00 6 1 10.0.0.1 0000.0000.0001 ubr10000#show cable qos profile 6 ID Prio Max Guarantee Max Max TOS TOS Create B IP prec. upstream upstream downstream tx mask value by priv rate bandwidth bandwidth bandwidth burst enab enab 6 1 64000 0 128000 0 0x0 0x0 cm no no The behavior was discover on a uBR10012 router running IOS 12.2(15)BC1b. The value seems to be incorrect only for the command <show cable profile (x)>. SNMP will verify correct parameters are being used: docsIfQosProfMaxUpBandwidth.1 docsIfQosProfMaxDownBandwidth.1 Workaround: Presently there is no workaround for this issue other then using SNMP.

Table 24 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed96250	UGS voice packets on a uBR10012 router may be delayed. This causes choppy voice in the US. There are no known workarounds.
CSCee00895	In the uBR10012 router, packets switched by PXF are counted as process switched packets for the backhaul interfaces. These erroneous counts are displayed in 'show interface switching' output. There are no known workarounds.
CSCee01374	The PRE may crash when multiple simultaneous config sessions are executed via VTY and HCCP is configured in the cable interfaces. There are no known workarounds.
CSCee01703	RP may crash with the use of particular config file. 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.
CSCee06180	On the uBR10012 router, cable line card 5x20S may get broken. At that instance all the communication between 5x20 line card and main processor is stopped and card disappeared from all show commands. The following message displayed in cmts console log `.... %IPCOIR-3-TIMEOUT: Timeout waiting for a response from slot x/y` Workaround: To recover cable line card, issue the following command **CMTS# hw-module slot x reset** Where x and y are slot and subslot numbers
CSCee09412	If LC switch over happen before PRE switch over and there is some CM in online(d) state, after PRE switch over, these CM online(d) are not in RP database and cannot be seen from PR. For example ping cannot be successful and SNMP poll cdxCmCpeEntry will fail. Workaround: Reset those CM online(d) by cli “clear cable modem <xxx> reset”.
CSCee12121	LED of DS ports at mc520s-d light up after reloading the uBR10012 router. However, **showdown** command was configured the DS ports. Workaround: Configure **no shutdown**, then LED is lights-out.
CSCin54055	DOCSIS1.0 Qos profile created by CM is not seen in “show cable qos profile” CLI output after PRE switchover. There are no known workarounds.

Table 24 Open Caveats for Cisco IOS Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCin56782	CMTS may crash when protector interface made shutdown and the HCCP configurations removal from the working interfaces. There are no known workarounds.
CSCin59835	CMTS may experience spurious memory access with RPR+ switch over. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC2

The caveats listed in Table 38 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 25 Closed and Resolved Caveats for Release 12.2(15)BC2

Caveat ID Number	Description

CSCdy76009	If a uBR10K cable line card is pulled, shutdown, or powered off, and the show controller is subsequently issued, the user sees "- Hardware is Removed" for the card when he should see (for example):
	`"Interface Cable7/0/1`
	`Hardware is UBR10000 CLC - Removed"`
	This incomplete output can be seen on any 12.2BC release through August 2003.
	There are no known workarounds, but the **show run | inc card** command will show all configured card types, which is similar in output.

CSCdz29957	The Last input param is only updated when a packet is punted for processing in the slow path. Last input param is not updated when packets are processed by the fast path. There are no known workarounds.
CSCdz85628	Unable to get the MIB value "cdrqCmtsCmStatusTable" from another SNMP agent. Workaround: Display the remote-query info from the command line using **show cable modem remote-query** command on CMTS.
CSCea08812	This problem shows up when running multicast over bundle interfaces. If a client leaves the multicast group the CMTS will continue to forward multicast traffic on that interface. This only causes a performance problem because unnecessary traffic is consuming the available bandwidth. There are no known workarounds.
CSCea41491	After a PRE switchover, the show cable modem vendor summary command may produce output inconsistent with the show cable modem summary command. There are no known workarounds.

Table 25 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. Workaround: Do not configure the IP address for the local pool.
CSCea80895	Reliability counter in 'show interface cable' decrease without error. Cisco IOS software version 12.2(11)CY. There are no known workarounds.
CSCea82892	“clear cable flap-list all save-counters” does not save the counters This issue is seen only in the uBR10012 router. There are no known workarounds.
CSCeb10426	The virtual interface featurette does not have SNMP support committed yet. FEAT-11252 is for SNMP support for virtual interface for MC520. With “cable upstream max-port N” where N > 4, the following SNMP tables/objects could possibly have problems (either missing entries, show extra entries, or report wrong value). There are no known workarounds.
CSCeb26908	The available downstream bandwidth value is not consistent among different CLI commands. There are no known workarounds.
CSCeb31490	uBR10012 router may reply with wrong source ip address 0.0.0.0 as the first hop for UDP based traceroute. There are no known workarounds.
CSCeb40129	Maximum DS throughput much below 10MB was observed for business subscribers with MIR configuration of 10Mbps because of tail drops in PXF queues. The packet drops will cause the TCP sessions to throttle back and so the throughput for these sessions will be lower than the MIR configured for the flow. This problem affects TCP sessions with high bandwidth downstream flows. There are no known workarounds.

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.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCeb48061	When a clear cab modem etc. is issued on the RP, an IPC is sent to the LCs. The LCs then mark the modems offline and send another IPC to the RP so that the RP can then mark the same modems offline. The following messages will appear: `UTC: %UBR10K-6-CM_INCONSISTENCY: CM state inconsistency 0000.395f.2259(msgp 0000.395f.2259), sid 206 (206), mac state 16, hwidb Cable5/0/4` On RP, modems would lose connectivity and go offline. It can occur during maintenance or configuration when the CLI (cle cable modem) is followed by a switchover There are no known workarounds.
CSCeb54879	This is a feature request is to have the ability to specifically clear ONLY the “cable modem hop” counters. Currently, the only way to clear the hop counters is the **clear counters** command, but this command also clears other counters which we'd like to avoid. There are no known workarounds.
CSCeb57822	If a frequency hop occurs immediately prior to switchover, all modems on one or more upstreams of the MC520S go offline. This is seen with switching to Protect and also while reverting back to the Working. Upstreams do not always recover and require a shut/no shut to clear the problem. There are no known workarounds.
CSCeb58851	The CMTS may display an error message, like the one below, when a **hw-module reset** command is issued: `SLOT 8/1: Jul  8 15:31:25.283: %SYS-3-CPUHOG: Task ran for 2104 msec (3/3), proc ess = CR10K CLC Delete all SIDs task, PC = 604258D4.` This may happen when several interfaces are down at the same time and there are a lot of modems attached to those interfaces.
CSCeb59073	N+1/BPI+ is not officially supported yet. There are no known workarounds.
CSCeb59781	When switchover the slave interface, the IGMP client on that interface may have multicast traffic lost. Workaround: Use “clear ip mroute *”

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
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 problem 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.
CSCeb62481	When PXF microcode crashes, PXF client writes a crashinfo onto bootflash: for future debugging purposes. In some cases "Tag debug data" in crashinfo could be useless. This issue is only a issue related to debuggability of a pxf crash. And doesn't affect router operation or any PXF functionality, as such. There are no known workarounds.
CSCeb67903	If an MC520S card receives a ranging request that is reported to be more than 4096Hz away from the desired upstream frequency, the MC520S card will command the modem in question to change it's upstream frequency in the wrong direction causing the modem to fall offline. This problem typically only affects cable modems with extremely poor upstream frequency calibration just after they initially come online or just after changing upstream channel characteristics. In some cases such modems with poor upstream frequency calibration may work better using lower upstream frequencies and wider channel widths. There are no known workarounds.
CSCeb68955	In rare circumstances, the PRE may crash after a line card switch-over. There are no known workarounds.

CSCeb69929	The following CLI will now be available for the uBR10012 router platform:
	`sh cr10k-rp cx/y/z <sid> [classifier | mac-rw-index | queue]`
	`sh cr10k-rp cx/y/z <sid> service-flow [ds | us]`
	`sh cr10k-rp cx/y/z queue [be | cir | llq]`
	There are no known workarounds.

CSCeb71752	Issuing a **show cable modem cable x/y/z summary** command might cause the PRE to crash with ubr10k-k8p6-mz.999-99.122BC_UB_030716 image. PRE fails over to secondary and the router recovers itself. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCeb73026	The CMTS may display the error below after an N+1 switch over. `HCCP 1 0 1: HCCP_ASSERT_EXT FAILED: line 3961 in ../src-4k-cr7200/cmts_hccp_msg.c` There are no known workarounds.
CSCeb75194	In the event of a MC520 line card crash, the N+1 Fast Fault Detection feature may not work. The switch over will be delayed for approximately 9 seconds, leading to a high probability that modems will go offline. The problem appears to happen on alternative switch overs. There are no known workarounds.
CSCeb76582	This fix ensures that the new tables defined in PXF for the VTMS mir fix CSCeb37891 are correctly initialized to zero. There are no known workarounds.
CSCeb76602	Spurious memory access may happen during HCCP config/unconfig. Workaround: Shut the Protect interface(s) associated with this HCCP group, then configure HCCP before re-enabling HCCP.
CSCeb77578	When the cable line card is hot swapped or plugin during run time, the upstream trap is missing. Workaround. Do not depend on the trap. Check the upstream ifOperStatus for the state.
CSCeb77720	Modems may stuck at init(o) when cable dynamic-secret is configured. There are no known workarounds.
CSCeb78298	Spurious memory access is observed on RP after copying startup (with N+1 config) to running config. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCeb78345	Under some circumstances, it may be observed that adding additional upstream ports to a previously active downstream channel causes certain modems to be unable to connect to the additional upstream channels. This problem may also be seen if additional upstreams are enabled some time after initial system startup, or if minislot sizes are different for different upstream channels on the same interface. When this problem is seen, the system stops providing initial ranging slots, or it only provides initial ranging slots in large intervals (e.g., several seconds). If upstream nodes are combined, and if load balancing is configured, the result may be an unstable condition, since the system will continuously attempt to move modems to the new (less loaded) upstream channels, and those modems may not be able to come online on the new upstream channel(s). For example, if three upstream channels (U0..U3) are active, and another upstream channel is added with no cable upstream 4 shutdown, the problem may be observed. It was also seen after adding four ports to an existing configuration, using the following commands on a cable interface. **cable upstream max-ports 8** **cable upstream 4 connector 4** **cable upstream 5 connector 5** **cable upstream 6 connector 6** **cable upstream 7 connector 7** In another instance, the problem was seen after the minislot-size was changed on an upstream channel. If this condition is seen, there are some possible workarounds: - issue a card reset with hw-module slot subslot <slot>/<card> reset - OIR the affected card - reboot the system There are no known workarounds without taking all modems on the affected card offline.
CSCeb85608	Some DS multicast packets were observed with CRC check failure when cable multicast-echo feature is turned on the CMTS. Workaround: Turn off cable multicast-echo feature interface command: no cable ip-multicast-echo

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec00765	If an upstream is assigned to a spectrum group which has freq band a little bit bigger than the channel-width (e.g. channel-wdith 3.2MHz and the band from 35-39MHz), upstream will hops to itself to avoid noise. It should change the modulation from QAM to QPSK because of the default hop priority is “f m c”. Workaround: Using a spectrum group with a bigger frequency band for frequencyhopping.
CSCec00865	ack39 is observed on certain upstream after running the cmts for 5 days. Modem on upstream with ack39 problem won't be able to display the CNR by CLI “sh cab modem cnr” and the spectrum management function is broken on this upstream. Workaround: CLI “test cab ack39 c7/1/0 u0” will take the upstream out of this problem.
CSCec07639	When DMIC is configured and a large number of cable modems attempt to connect to the CMTS at the same time, the system may experience high CPU utilization and the modem may have trouble going past state init(o) and may even reset and re-range. The problem is particularly severe when a large number of Cisco cable modems are connected to the system and the config file is greater than 4096 bytes in size. Workaround: Disable DMIC. Alternative workaround: Edit the config file so that it is less than 4096 bytes in length.

CSCec14598	The router does not transmit RADIUS packets to a RADIUS server when information regarding which radius server to use is downloaded via a protocol other than RADIUS.
	This issue only occurs 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:
	`<CmdBold>radius-server host`
	`<CmdArg>x.x.x.x<NoCmdArg><noCmdBold>`
	Where 'x.x.x.x' is an arbitrary ipv4 address.

CSCec17473	After abnormal traffic pattern on cable interface, the “CR10K Request di” process increased by ~54 MB in “show proc cpu”. Determined that buffers that overflow receive ring for process, were never freed. Workaround: Event does not appear frequent, only 1 incident in 22 weeks of uptime. However there is no known workaround to recover lost memory. System continued to run without incident following one time event.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec19196	Some CPE's may loose IP connectivity after installing IOS 12.2(15)BC1 on a uBR10012 router router. This problem occurs when a cable subinterface is configured for **cable-source-verify [dhcp]**. Workaround: Remove **cable source-verify [dhcp]** on the cable subinterface or entering **clear cable modem <mac> delete** for affected Cable Modems restores IP connectivity.
CSCec22551	Packets from high bandwidth multicast streams can be dropped in the uBR10012 router when it is operating in the best-effort flow aggregation mode. There are no known workarounds.
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.
CSCec23439	The cable MAC layer ifInOctets will include the CRC bytes. There are no known workarounds.

CSCec25534	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"`
	Workaround: None. 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"`

CSCec26556	When configure cable qos enforce-rule without no-persistence, the enforced QoS profile does not work correctly in force when a cable modem reboot. Looks good regarding **show cable modem xxxx qos** command, but in fact, the traffic go through higher than MaxSusRate of enforced QoS profile. This occurs on a Cisco IOS software version 12.2(15)BC1 "cable qos enforce-rule" is configured. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
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.
CSCec30612	When a CM is reset either from the CMTS or the CM itself, if the CM is using a docsis 1.0 qos profile, the reset is not propagated from the CLC to the RP. There are no known workarounds.
CSCec30869	If the first cable interface is admin shutdown, when show cable modem CLI is typed on the PRE, the title header associated with the CLI output is not shown. There are no known workarounds.

CSCec35575	Cisco Ubr10000 Cable linecard may crash in rare occasions with the following messages:
	`SLOT 5/1: 00:00:34: %UBR10000-5-UPDOWN: Interface Cable5/1/4 Port U0, changed state to administratively down`
	`SLOT 5/1: 00:00:34: %UBR10000-5-UPDOWN: Interface Cable5/1/4 Port U1, changed state to administratively down`
	`SLOT 5/1: 00:00:34: %UBR10000-5-UPDOWN: Interface Cable5/1/4 Port U2, changed state to administratively down`
	`SLOT 5/1: 00:00:34: %UBR10000-5-UPDOWN: Interface Cable5/1/4 Port U3, changed state to administratively downCMD: 'end' 08:31:19 UTC Wed Sep 17 2003`
	`%ALIGN-1-FATAL: Illegal access to a low address addr=0x1C, pc=0x6041F320, ra=0x6041EFC8, sp=0x6129C6B8`
	`%ALIGN-1-FATAL: Illegal access to a low address addr=0x1C, pc=0x6041F320, ra=0x6041EFC8, sp=0x6129C6B8`
	`Unexpected exception, CPU signal 10, PC = 0x6041F320`
	`-Traceback= 6041F320 6041C288`
	`$0 : 00000000, AT : 0300FE00, v0 : 00000000, v1 : 00000000`
	`a0 : 619489BC, a1 : 61944BF4, a2 : 00000000, a3 : 00000051`
	`t0 : 00000400, t1 : 3E800010, t2 : 00000001, t3 : 00000008`
	`t4 : 3400F900, t5 : 00000000, t6 : 00000000, t7 : 00008000`
	`s0 : 00000000, s1 : 00000000, s2 : 00000000, s3 : 61250C40`
	`s4 : 607A0000, s5 : 00000000, s6 : 61942B18, s7 : 607A0000`
	`t8 : 0D0D0D0D, t9 : 00000004, k0 : 00000000, k1 : 00000000`
	`gp : 60E24AA0, sp : 6129C6B8, s8 : 60F30000, ra : 6041EFC8`
	`EPC : 6041F320, ErrorEPC : FFFFFFFF, SREG : 3400F903`
	`MDLO : 22E0C319, MDHI : FE541066, BadVaddr : 0000001C`
	`Cause 0000000C (Code 0x3): TLB (store) exception`
	There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec39692	Cisco uBR10012 router running 12.2(11)BC2 may crash. Conditions: This symptom is observed on a Cisco uBR10012 router 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.
CSCec44859	If the failure case is Keepalive failure when configure N+1/MC520 on uBR10012 router, the DS0,1,2,3 interfaces automatically revert back to the working interface from the protect interface This issue occurs on Cisco IOS software version 12.2(15)BC1. There are no known workarounds.
CSCec45384	When using 20ms packetization rate, some of the calls made are dropping packets. This happens with some MTAs. There are no known workarounds.
CSCec45453	In HCCP environments, uBR10012 router and the 5x20 card, the wrong IPCup/down notifications appear when experiencing IPC memory leak/trace/card reload running 12.2(15)BC. There are no known workarounds.
CSCec47470	A uBR10012 router may crash with an error message similar to %ALIGN-1-FATAL: Illegal access to a low address. There are no known workarounds.
CSCec47748	If the first cable interface is admin shutdown, when show cable modem CLI is typed on the PRE, the title header associated with the CLI output is not shown. There are no known workarounds.
CSCec48387	Gates at committed states for active voice call can be stuck after LC OIR. There are no known workarounds.
CSCec54694	After several weeks of uptime, cable modem traffic is not being correctly routed to the DHCP server configured as helper-address. This problem occurs when tag-switching (MPLS) is enabled on the backhaul GigE interface. Workaround: Use clear ip route <address of DHCP Server>
CSCec55868	On the uBR10012 router, it is possible that high priority traffic can be dropped on the 5x20 linecard because the back pressure mechanism to throttle PXF is not working. This is only a problem during link congestion. There are no known workarounds.
CSCec56459	In VPN setting, when do "show pxf cable source-verify", there are zero empty entries shown. It does not affect the functionality of cable source-verify. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec57929	On uBR10012 router, with bundling configured, when the cable linecard containing the bundle master is removed followed by a 'no card' command, the RP may print an error message: `%GENERAL-3-EREVENT: cmts_update_sid_vcci:No if_info on hw CableX/Y/Z idb CableA/B/C.D while linking sid <SID>` Workaround: Remove bundling configuration on the master interface and reapply.
CSCec61676	When cable intercept is enabled, those intercepted packets show to have extra bytes appended and this causes replay problem on CALEA server. There are no known workarounds.
CSCec62085	Per CPE access-lists do not work on the uBR10012 router. There are no known workarounds.
CSCec63086	Show cable flap list can crash due to memory depletion. There are no known workarounds.
CSCec65787	show proc mem sorted may crash the router with a large number of modems. Workaround: Use show proc mem.
CSCec67809	Investigating potential memory leak in DHCPD Receive process. Monitor “show process memory”, Process 111 indicates Memory Held increasing every day. There are no known workarounds.
CSCec68998	Per interface diversion counts are not available in uBR10012 router. Further the number of these packets being enqueued to the process level is also not available through any show command. There are no known workarounds.

CSCec73238	When CM or CPE comes up through DHCP on VPN subinterface, the FIB index in the cable source verify table is zero. (use “show hardware pxf cable source-verify” to show).
	For example:
	`router#sh hard pxf cable source-verify 10.2.3.4`
	`IP Address Interface FIB Index Mac-Domain SID`
	`10.2.3.4 Cable6/0/0.7 0 2 3`
	`10.2.3.4 Cable6/0/0.2 1 4 4`
	This causes the entry cannot be removed even when the CM or CPE is no longer exist.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCec76205	A PRE switch-over to the Standby PRE fails with 34,000 modems on the uBR10012 router. The process takes 5 minutes and line cards reset and modems do not come online. Successful switch-overs have been performed with 10K-15K modems at other sites. It's unknown what the modem limit is. Workaround: Reset the Line-cards manually to bring modems back online.
CSCec83212	During modem registration the Active PRE will consume all IO memory when the modem count reaches 27K-29K. This problem is specific to 12.2(15)BC1a. There are no known workarounds.
CSCec83821	The CMTS may fail to register modems correctly when the TFTP-Enforce command is enabled. The CMTS may display the message below. `%UBR10000-4-REGISTRATION_BEFORE_TFTP_MARK: Registration request unexpected: Cable Modem did not attempt TFTP. Modem marked with #. CM Mac Addr <xxxx.xxxx.xxxx>` There are no known workarounds.
CSCec85777	This bug is used to release a new 5x20 MAC chip firmware version. There are no known workarounds.
CSCec85800	This bug was filed to release certain debugging capabilities in the PXF. There are no known workarounds.
CSCec87802	High cpu utilization mostly due to CEF Scanner. This issue is observed on a uBR10012 router series that is running IOS 12.2(15)BC1. There are no known workarounds.
CSCec89558	MC5x20 line-card to line-card communication may fail. There are no known workarounds.
CSCed02703	Background statistics collection called from the CEF process is consuming high CPU levels on the RP when the CMTS is in steady state. There are no known workarounds.
CSCed03064	SNMP ENGINE process CPU usage is triggered by external MIB objects query. As long as there are one or many network management system querying the CMTS for some MIB objects, the SNMP ENGINE process will consume some CPU usage as SNMP ENGINE process is normal priority process. Querying ifTable could cause high CPU spike. For example, getting the whole ifTable with get next command could cause high CPU spike above 30% in 35K CMs system with total CPU load around 75%. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed03085	On a uBR10012 router, when a CPE is disconnected and the corresponding ARP entry times out, some internal structures may not be reclaimed until the mac rewrite index pool is depleted and indices are reclaimed and reused. As a result, the DHCPD process can show up as holding a large amount of memory (in the order of 10 MB). Workaround: shut/no shut the cable interfaces.
CSCed07613	If a gate-delete message is received from CMS, the gate state and service flow on the RP are cleaned up, but corresponding toaster resources may not be cleaned up. If several such gate-delete messages are received, it may eventually exhaust toaster resources, resulting in QALLOC failures. There are no known workarounds.
CSCed09930	A Cisco Universal Broadband Router may reload unexpectedly as a result of its memory getting corrupted. This issue occurs only when using the CMTS remote query feature. Workaround: Disable the remote query by no cable modem remote-query.
CSCed10755	The cable source-verify md sid entry cannot be removed if there are 2 or more CMs/CPEs come up from different VPNs and acquire the same ip address. (shown by “show pxf cable source-verify <ip>”). This would not affect the cable source-verify functionality, however, would cause scalability issue when all the entries are used up. There are no known workarounds.
CSCed11279	The PRE may crash under some load conditions. There are no known workarounds.
CSCed12910	During continuous operation of the uBR10012 router, it is possible that an odd numbered downstream on the 5x20 linecard gets stuck, causing all the CMs to go offline. The corresponding even numbered downstream, will lose IP connectivity as a result. As a result on the even numbered downstream CMs that try to reregister will get stuck in init(i) state. To recover from the problem, you need to reload the linecard. There are no known workarounds.
CSCed16691	PXF internal packet memory for a certain linecard may get stuck after a uBR10012 router boots up. This will cause all packets coming into that linecard to get dropped. When RP detects that PXF IPM is stuck by default it will print a PXF_DMA-3-FBB_LINE_CARD error message If packet drops are observed one can recover by executing the **microcode reload pxf** command. Automatic PXF reload can be configured using the **exception pxf ipm** command in the global configuration. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed17260	In VPN environment, when there are CMs/CPEs getting the same ip address in different subinterfaces, a newly added source-verify entry with the same ip address may overwrite the previous CMs/CPEs source-verify entries. This does not cause any connectivity problem, however, will cause performance and scalability issues. There are no known workarounds.
CSCed17487	If we have around 44K modems on a uBR10012 router, it may take up to 9 minutes for the PRE failover to complete. There are no known workarounds.
CSCed21069	The secondary PRE crashes while receiving the msg to clear its inter-db when a clear cab modem all reset is done on the primary PRE. The crash is due to trying to free mem for RP DS srv flow which is already NULL. This crash seems to be occurring when the RP DS srv-flow has failed to be added to the inter-db during the bulk/dynamic sync for a modem. There are no known workarounds.
CSCed21438	The CMTS rewrites the IP source of the DHCP OFFER to the pc client and changes it to the PRIMARY subnet on the Cable interface which breaks ACL's that are installed in the CM DOCSIS config file. This is when running "cable dhcp-giaddr policy" where the relay-agent is smart enough to decide how to populate the giaddr with the correct subnet depending whether the BROADCAST is coming from a PC or cable modem. The CMTS is following the rule according to RFC 1542 with regards to the giaddr, yet the spec does NOT specify clear cut rules for the source IP address of the packet. Cisco implementation rewrites the IP Source to the cable modem subnet during the OFFER. This is not wrong but under certain conditions where security filters reside in the DOCSIS config file get broken. There are no known workarounds.
CSCed22172	The keepalive status was not displayed in the output of sh int cable x/y/z. The keepalive status is only displayed at the level of the Line Card. 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
CSCed29742	CLI Command "cable downstream rf-power" disappears from show run under the HCCP protected interface. This happens only when the interface that is configured as "Protected" is in working status, and an incident happens (or HCCP switch over is forced) that causes the interface to revert back to standby status. There are no known workarounds.
CSCed31927	During a PRE switch-over, a IPC trace-back may be noticed with a high number of modems. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed45790	Under certain circumstances, Cable Modem data in CLC and RP may be out of sync. If this happens, especially when the RP has a SID associated with the modem, but the CLC starts to use a different SID, the modem in question will no longer be able to register and be stuck in offline mode. Visible effect to the user is that affected modems either do not show up at all, or always show up as offline. Workaround: shut/no shut affected interfaces or to switch to a backup interface if HA is active.
CSCed46705	Running config never get hccp-xxx extensions from startup-config. Workaround: You have to configure the CLIs from startup everytime router is loaded.
CSCed49070	The standby PRE could reload during boot up due to inconsistencies. No action is required by the user. 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.
CSCed53178	ENTITY-MIB changes to support Virtual Interface.
CSCed55021	A CMTS with a large number of cable modems connected may exhibit high CPU in the DHCPD Receive process as many cable modems all attempt to come online. As modems come online successfully, the CPU utilization will gradually decrease. This issue may be exacerbated by having an unusually large number of secondary IP addresses configured on cable interfaces. Workaround: Reduce the number of secondary IP addresses configured on a cable interface. Alternative workaround: Deliberately reduce the rate at which cable modems may come online by manually increasing the cable insertion-interval to a large value such as 250 or 500ms.
CSCed55652	When CIR flows are being used in a uBR10012 router, certain race conditions that can occur while configuring queues may result in lowered performance for flows on affected downstreams. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed60116	CSCed51052 reported high CPU usage by cmts source-verify code. This DDTS was created to optimize CMTS src verify for IP and ARP lookup as well as improve all CMTS hash bucket entry linear walks. There are no known workarounds.
CSCed60220	A memory leak occurs in the *Dead* process on the PRE. Workaround: Disable AAA Exec Accounting and Network accounting.
CSCed65223	Similar problem has been reported in CSCea05180 for the 10K routers. However, UBR10000 is also seeing the same problem. Basically, 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.
CSCed65409	Bogus ARP entries are created when multiple DHCP servers reply with their offers. This can significantly increase memory consumption when many CMs are trying to register. It also causes the router to perform unnecessary arp entry addition. This is a result of bad sync. There are no known workarounds.
CSCed68829	Some modems might not be queried from SNMP cdxCmCpeTable and linecard CLI “show cable device access-group”. Workaround: shut/no shut the cable interface.
CSCed68879	Running 12.1(15)BC1b, and noticed that for some of his MC16S cards, snmp returns a value for docsIfSigQSignalNoise that seems about 1000x higher than expected, whereas CNR measurement on the interface shows that noise is in range. Workaround: Use the CNR value from **show interface cable** command line output rather than snmp response from docsIfSigQSignalNoise for problem determination.
CSCed70180	Certain modems, when configured in routing mode, might not be able to pass IP traffic when DMIC is enabled on the CMTS with IOS version 12.2(15)BC1b. The cable modem is able to ping the directly connected interface on the CMTS but it cannot ping beyond the CMTS. An extended ping from the CMTS to the cable modem RF interface also fails. Workaround: Disable DMIC on the CMTS.
CSCed72979	Cable Line Cards may become unresponsive under certain conditions. If this happens, the card will go offline, but it will not reboot itself. It has to be reset manually using the **hw-module reset** command. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description

CSCed76837	If there are lots of CM/CPE in the linecard, the SNMP query MIB tables related the CM/CPE info will possibly have SNMP-3-CPUHOG message and trackback. Also the CM/CPE may have connection problem (drop offline or lose VPN).
	The MIB tables are listed below. They are all invoke the same API to get the sorted table which the entry is searched.
	`CISCO-DOCS-EXT-MIB:cdxCmCpeTable,`
	`DOCS-IF-MIB:docsIfCmtsMacToCmTable`
	`DOCS-QOS-MIB:docsQosCmtsMacToSrvFlowTable`
	`CISCO-DOCS-REMOTE-QUERY-MIB:cdrqCmtsCmStatusTable`
	After fix:
	– All the SNMP query for above tables will get info from RP/NPE only. So LC will not be affected.
	– The SNMP query Get EXACT will have real time response.
	– SNMP Get NEXT for above MIB tables is too expensive in a big system since it needs to go through whole CM/CPE in order to know which CM/CPE is the next entry of the query. Users are recommended to use SNMP GET EXACT to retrieve the info for a specific device.
	In order to prevent CPU spiking for GET NEXT for above MIB tables, In the CMTS which number of devices (CM/CPE) is greater than 1000, the SNMP query GET NEXT will not get any entries returned. GetBulk has also the same problem as GetNext since internally, it searches for the next entry.
	There are no known workarounds.

CSCed79616	Specific running configuration may not be synched to the Standby PRE. After switch-over, behavior is cannot be predicted. Workaround: Do not configure the CMTS from multiple VTY sessions.
CSCed83401	This problem is found by reviewing the code. Whether it happens and what form it takes is unknown. There are no known workarounds.
CSCed83593	Dangling DS service flows. This issue occurs on LC switchovers. There ar e no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCed84052	On the uBR10012 router, the throughput for a backhaul queue can decrease significantly intermittently. This problem will rectify itself when the affected queue or some other queue on that affected link becomes active (packets get enqueued to an empty queue) or becomes inactive (queue is drained and becomes empty. This problem is less of an issue in the production environment where the pair of default queues on the GigE are continuously being used and so are going active and inactive. If instead, there are 2 GigE links with the backhaul routes being equal cost paths, only one queue will be used per GigE link so that the chance of another queue coming active is lower. Even in this case, when the high priority queue goes active or inactive due to routing protocol traffic, the problem will be fixed automatically.

CSCed87070	A ubr10000 Series router with mc5x20 cards may produce the following error when Spectrum Groups are added
	
	`router#cable upstream 1 spectrum-group 14`
	`Mar 3 10:17:07.213: %UBR10000-3-NOMEM: No more inuse sets.`
	`router#cable upstream 1 spectrum-group 14`
	`Mar 3 10:17:07.213: Cable5/0/0 U1: shared attach failed`
	
	`CPU subsequently spikes to 90% mostly in the interrupt context.`
	
	A reload may be required in order to recover.
	
	There are no known workarounds.

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.
CSCed91422	The RP CPU on a uBR10012 router can go to 100% while handling invalid packets being sent from the CPEs on the upstream when source-verify or source-verify dhcp is configured. There are no known workarounds.
CSCed92381	This issue will happen if each cable interface of a Cable line card does not share the same TEK lifetime. Workaround: Make all cable interfaces of a Cable line card share the same TEK lifetime.
CSCee03345	If on a system with hccp configured, the protect line card crashes and then hangs during crashinfo collection, it may lead to sync-pulse failure on all the other working line cards and followed by power cycle of all the working line cards. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCee11695	When the CMTS is configured with “cable source-verify dhcp”, and bundling is configured, and ip pkts from CPE are being source verified, the lease query response may be incorrectly dropped, leading to the CMTS continuously sending lease query requests and dropping lease query acks. There are no known workarounds.
CSCin36219	The max cpe configurations are not synched to the Standby PRE. After a PRE switch-over, the max cpe configurations will be set to unlimited. There are no known workarounds.
CSCin36271	Cable filter groups are persistent through a PRE switch-over. Workaround: Reconfigure the cable filter groups after switch-over.
CSCin41164	If a packet has more than 60 bytes suppressed by PHS, CMTS fails to properly restore the packet. This bug does not affect JIB based line card such as MC520S, MC520U and TransAm. In the first 64 bytes of a packet, it contains two bytes IP checksum, and another two bytes for TCP or UDP checksum. So, it is not likely a problem in customer sites to have more than 60 bytes suppressed by PHS. There are no known workarounds.
CSCin46501	Ping from CPE to CMTS fails under certain conditions, when source verify is configured. Ping from CPE to CMTS fails under the following scenario. 1. Create a sub-interface over a bundled interface 2. Configure “cable source-verify” on the new subinterface and assign primary and secondary address pools 3. Bring up a CPE using DHCP on the subinterface 4. Now change the CPE from DHCP-assigned address to static IP address from the secondary pool. Ping from CPE to CMTS fails. Workaround: Remove “cable source-verify” from the subinterface above.
CSCin46885	CMTS does not allow CM to register with DOCSIS1.1 configuration file with DMIC enabled scenario for the CM which is already marked. Workaround: Remove the marking by “clear cable modem ? lock” or “clear cable modem ? delete” at CMTS and make the CM to came operational with DOCSIS1.1 configuration file.
CSCin48221	When a rogue CM is displayed in show cable modem rogue, the spoof count is a negative number and a junk dynamic secret is being displayed when none was configured. There are no known workarounds.

Table 25 Closed and Resolved Caveats for Release 12.2(15)BC2 (continued)

Caveat ID Number	Description
CSCin48325	This problem happens when a cable interface is configured as an HCCP protect. And then if a user configures the 1st sub-interface on the interface, the interface line state after configuration will stay down, and never comes as up, until a shut-no-shut is done, after which line protocol state comes up. This does not happen when adding a second or more sub-interfaces.
CSCin49976	The packets received counters of native vlans in the output of "show vlan" may shoot up to very high unexpected values after a "clear vlan statistics" is done. The problem is created by re-configuring an existing VLAN to act as the Native VLAN. The work around is to delete the existing VLAN first then add it back in as the Native VLAN. There are no known workarounds.
CSCin50315	When "cable shared-secret" is not configured and "cable dynamic-secret" is configured, the "cable secondary-shared-secret" is not ignored. There are no known workarounds.
CSCin50638	Redundant CLI options shown under <show hardware?>. There are no known workarounds.
CSCin63379	"IP Protocol Type" missing from the classifier lists after done N+1 switchover. Classifier was added to the Service flow by DSC msg from CM. There are no known workarounds.
CSCuk44928	When you save a configuration first to the standby Performance Routing Engine (PRE) and then to the active PRE, the configuration may not be saved and the following error message may be generated: `startup-config file open failed (Device or resource busy)` This issue is observed on a Cisco 10000 series and c7500, that is configured with redundant PREs and that runs Cisco IOS Release 12.0(26)S. The symptom may also occur in other Cisco IOS releases. 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 38 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 26 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 38 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 27 Closed and Resolved Caveats for Release 12.2(15)BC1f

Caveat ID Number	Description
CSCed23795	During reload of a uBR10012 router, a traceback is seen. There are no known workarounds.

CSCed71560	uBR10012 router running 15BC1b fails dhcp for CPE inside a Motorola DCT5000 when no bundle entry is found for an incoming dhcp packet.
	This issue is restricted to only such settop boxes - modems always come online ok on the same uBR10012 router and cable line card.
	Workaround: Perform the following steps:
	1. Feed the failing DCT CPE mac addr to the following CLI:
	`sh ip arp vrf internet <CPE mac addr>`
	The CLI output will give you the cable interface(s) that has to be cleaned up for offending IP addr entries in the CMTS bundling table.
	2. To find out offending IP entries in the CMTS bundle table, use the CMTS hidden CLI of:
	`sh int cx/y/z buck rp`
	Any “host” entry in the output that has the IP field “unavailable” is an offending entry. This entry has to be removed from the CMTS by invoking:
	`clear cable host <offending IP's mac addr>`
	3. Once all offending CMTS bundle entries are removed, reload the modem in the DCT5000 and now both modem and CPE will show up as registered on the CMTS.

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.
CSCee84392	In a MPLS/VPN environment cable modem using DOCSIS 1.0 becomes unreachable. The CPE attached to it is still reachable. This issue has been detected while reseting the modem. The sub-interface where the MOdem is assign to, is configure with “cable source-verify dhcp” and “no cable arp”. Workaround: Make sure “no cable arp” is unconfigured from the sub-interface default is “cable arp”.

Table 27 Closed and Resolved Caveats for Release 12.2(15)BC1f (continued)

Caveat ID Number	Description
CSCef04614	This improves cable modem bringup performance on a uBR10012 router. There are no known workarounds.
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.

CSCef44517	Immediately after booting up, a PRE-1 may unexpectedly reload with the following error:
	`%ERR-1-GT64120 (PCI-1): Fatal error, PCI retry counter expired`
	`GT=0xB4000000,`
	`cause=0x00001000,`
	`mask=0x00D01D00, real_cause=0x00001000`
	`bus_err_high=0x00000000,`
	`bus_err_low=0x00000000,`
	`addr_decode_err=0x00000470`
	The fault is limited to PRE-1 version 08 with Texas Instrument PCI bridge chips. This version can be identified by the Top Assy. Part Number visually (on the box) or in the show chassis CLI command:
	`Top Assy. Part Number : 800-17437-08`
	`^^^`
	Workaround: Upgrade IOS to 12.2(15)BC1e or higher.
	Alternative workaround: Upgrade IOS to 12.2(15)BC2d or higher.

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

Table 27 Closed and Resolved Caveats for Release 12.2(15)BC1f (continued)

Caveat ID Number	Description
CSCef49769	The 2x8 LC on the uBR10012 router can run very high CPU utilization for moderate amounts of upstream traffic. LCP1 is more susceptible than LCP2 due to lower base CPU performance. The 5x20 LC is not affected by this issue. This can cause box-wide issues as the LC throttles the PXF severely. Workaround: Reduce load on the affect linecard by moving CMs to a different LC. If you have an LCP1 based 2x8 linecard, replace with LCP2 Replace 2x8 linecard with 5x20 linecard.
CSCef52235	uBR10012 router running either 12.2(15)BC2c or 12.2(15)BC1b will run into the following issues when a 2x8 LC is running at 100% CPU. 1. No telnet access, only the console port works. 2. Modems that are online cannot come back online, the get stuck in init(rc). 3. Message that is being seen when the CMTS becomes unreachable: `%C10KEVENTMGR-1-MINOR_FAULT: PXF DMA Full OCQ Wait Error` 4. Trafiic slowing down for all the linecards, especially the backhaul interfaces. The issue was seen on a uBR10012 router with 16,000 CM's. Workaround: Reduce load on the LC running at 100% CPU. Alternative workaround: Reload the PXF microcode.

Open Caveats for Release 12.2(15)BC1e

This section documents possible unexpected behavior by Cisco IOS Release 12.2(15)BC1e 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)BC1e.

Closed and Resolved Caveats for Release 12.2(15)BC1e

The caveats listed in Table 38 are resolved in Cisco IOS Release 12.2(15)BC1e. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 28 Closed and Resolved Caveats for Release 12.2(15)BC1e

Caveat ID Number	Description

CSCef44517	Immediately after booting up, a PRE-1 may unexpectedly reload with the following error:
	`%ERR-1-GT64120 (PCI-1): Fatal error, PCI retry counter expired`
	`GT=0xB4000000,`
	`cause=0x00001000,`
	`mask=0x00D01D00, real_cause=0x00001000`
	`bus_err_high=0x00000000,`
	`bus_err_low=0x00000000,`
	`addr_decode_err=0x00000470`
	The fault is limited to PRE-1 version 08 with Texas Instrument PCI bridge chips. This version can be identified by the Top Assy. Part Number visually (on the box) or in the show chassis CLI command:
	`Top Assy. Part Number : 800-17437-08`
	`^^^`
	Workaround: Upgrade IOS to 12.2(15)BC1e or higher.
	Alternative workaround: Upgrade IOS to 12.2(15)BC2d or higher.

Open Caveats for Release 12.2(15)BC1d

All the caveats listed in Table 37 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 29 Open Caveats for Cisco IOS Release 12.2(15)BC1d

Caveat ID Number	Description

CSCdy76009	If a uBR10012 cable line card is pulled, shutdown, or powered off, and the **show controller** is subsequently issued, the user sees "- Hardware is Removed" for the card when he should see (for example):
	`"Interface Cable7/0/1`
	`Hardware is UBR10000 CLC - Removed"`
	This incomplete output can be seen on any 12.2BC release through August 2003.
	There are no known workarounds, but the **show run | inc card** command will show all configured card types, which is similar in output.

CSCdz29957	The Last input param is only updated when a packet is punted for processing in the slow path. Last input param is not updated when packets are processed by the fast path. There are no known workarounds.
CSCea08812	This problem shows up when running multicast over bundle interfaces. If a client leaves the multicast group the CMTS will continue to forward multicast traffic on that interface. This only causes a performance problem because unnecessary traffic is consuming the available bandwidth. There are no known workarounds.
CSCea41090	On a uBR10012 router running Cisco IOS Release 12.2(11)CY or Cisco IOS Release 12.2(11)BC3, configured with bundling, IGMP messages received on the upstream will be echoed back on all the downstreams of the cable bundle instead of only those that have previously received IGMP joins. There are no known workarounds.
CSCea41491	After a PRE switchover, the **show cable modem vendor summary** command may produce output inconsistent with the **show cable modem summary** command. There are no known workarounds.
CSCea80895	Reliability counter in "show interface cable" decrease without error. This issue may occur on a Cisco IOS software version 12.2(11)CY. There are no known workarounds.
CSCea82892	The **clear cable flap-list all save-counters** command does not save the counters. This issue is seen only in uBR10012 router. There are no known workarounds.

Table 29 Open Caveats for Cisco IOS Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCeb26908	The available downstream bandwidth value is not consistent among different CLI commands. There are no known workarounds.
CSCeb48061	When a clear cab modem etc... is issued on the RP, an IPC is sent to the LCs. The LCs then mark the modems offline and send another IPC to the RP so that the RP can then mark the same modems offline. The following message would then be encountered, and the RP. Modems would lose connectivity and go offline: `UTC: %UBR10K-6-CM_INCONSISTENCY: CM state inconsistency 0000.395f.2259(msgp 0000.395f.2259), sid 206 (206), mac state 16, hwidb Cable5/0/4` This issue may occur during maintenance or configuration when the CLI (cle cable modem) is followed by a switchover. However, this is a rare occurrence. There are no known workarounds.
CSCeb59073	N+1/BPI+ is not officially supported yet. There are no known workarounds.
CSCeb59781	When using switchover on the slave interface, the IGMP client on that interface may have multicast traffic lost. Workaround: Use “clear ip mroute *”.
CSCeb67903	If an MC520S card receives a ranging request that is reported to be more than 4096Hz away from the desired upstream frequency, the MC520S card will command the modem in question to change it's upstream frequency in the wrong direction causing the modem to fall offline. This problem typically only affects cable modems with extremely poor upstream frequency calibration just after they initially come online or just after changing upstream channel characteristics. In some cases such modems with poor upstream frequency calibration may work better using lower upstream frequencies and wider channel widths. There are no known workarounds.
CSCeb76602	Spurious memory access may happen during HCCP config/unconfig. Workaround: Shut the Protect interface(s) associated with this HCCP group, then configure HCCP before re-enabling HCCP.
CSCeb77578	When the cable line card is hot swapped or plugin during run time, the upstream trap is missing. Workaround. Do not depend on the trap. Check the upstream ifOperStatus for the state.
CSCeb78298	Spurious memory access is observed on RP after copying startup (with N+1 config) to running config. There are no known workarounds.

Table 29 Open Caveats for Cisco IOS Release 12.2(15)BC1d (continued)

Caveat ID Number	Description

CSCec14598	The router does not transmit RADIUS packets to a RADIUS server when information regarding which radius server to use is downloaded via a protocol other than RADIUS.
	This issue only occurs 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:
	`<CmdBold>radius-server host`
	`<CmdArg>x.x.x.x<NoCmdArg><noCmdBold>`
	Where 'x.x.x.x' is an arbitrary ipv4 address.

CSCec30612	When a CM is reset either from the CMTS or the CM itself, if the CM is using a docsis 1.0 qos profile, the reset is not propagated from the CLC to the RP. There are no known workarounds.
CSCec30869	When “show cable modem CLI” is typed on the PRE, the title header associated with the CLI output may not be shown if the first cable interface is admin shutdown. There are no known workarounds.
CSCec44859	If the failure case is a Keepalive failure when configure N+1/MC520 on uBR10012 router, the DS0,1,2,3 interfaces automatically revert back to the working interface from the protect interface. This issue occurs on Cisco IOS software version 12.2(15)BC1. There are no known workarounds.
CSCec47748	When reloading the 7200, if a uBR10012 router is connected to a 7200 (NPE-G1) gig interface, the uBR10012 router will be able to ping the 7200, but the 7200 can not ping the uBR10012 router. Workaround: Reload the uBR10012 router.
CSCec48387	Gates that are in committed states for active voice call may be stuck after LC OIR. There are no known workarounds.
CSCin36219	The max cpe configurations are not synched to the Standby PRE. After a PRE switch-over, the max cpe configurations will be set to unlimited. There are no known workarounds.
CSCin36271	Cable filter groups are persistent through a PRE switch-over. Workaround: Reconfigure the cable filter groups after switch-over.

Table 29 Open Caveats for Cisco IOS Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCin41164	If a packet has more than 60 bytes suppressed by PHS, CMTS fails to properly restore the packet. In the first 64 bytes of a packet, it contains two bytes IP checksum, and another two bytes for TCP or UDP checksum. So, it is not likely a problem in customer sites to have more than 60 bytes suppressed by PHS. This issue does not affect JIB based line card such as MC520S, MC520U and TransAm. There are no known workarounds.
CSCin46885	CMTS does not allow CM to register with DOCSIS1.1 configuration file with DMIC enabled scenario for the CM which is already marked. Workaround: Remove the marking by using “clear cable modem ? lock” or “clear cable modem ? delete” at CMTS and make the CM to came operational with DOCSIS1.1 configuration file.
CSCin48221	When a rogue CM is displayed in show cable modem rogue, the spoof count is a negative number and a junk dynamic secret is being displayed when none was configured. There are no known workarounds.
CSCin48325	When a cable interface is configured as an HCCP protect and the 1st sub-interface on the interface is configure, the interface line state after configuration will stay down and will not come as up until a shut-no-shut is performed, after which the line protocol state comes up. This issue does not occur when adding a second or more sub-interfaces. There are no known workarounds.
CSCin49976	The packets received counters of native vlans in the output of “show vlan” may shoot up to very high unexpected values after a “clear vlan statistics” is done. This issue occurs when re-configuring an existing VLAN to act as the Native VLAN. Workaround: Delete the existing VLAN first and then add it back in as the Native VLAN.
CSCin50638	Redundant CLI options are shown under <show hardware?>. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC1d

The caveats listed in Table 38 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 30 Closed and Resolved Caveats for Release 12.2(15)BC1d

Caveat ID Number	Description
CSCec55121	If an N+1 line card switchover has been performed at the Primary PRE, this bug could erroneously cause the HCCP state machine to be functional on the Secondary PRE. Because of mismatch of internal states, the PRE could crash while it is secondary or after a PRE switchover has been performed (and this Secondary PRE is changing states from Secondary to Primary). There are no known workarounds.
CSCed20369	On a uBR10012 router, if the VTMS queues that are assigned to CMs have an qid in the range of 28K to 32K, these queues can suffer from poor performance. Further, if these queues get deleted (CM goes offline), then PXF may crash because of the TBB length error. There are no known workarounds.
CSCed60116	CSCed51052 reported high CPU usage by cmts source-verify code. This DDTS was created to optimize CMTS src verify for IP and ARP lookup as well as improve all CMTS hash bucket entry linear walks. There are no known workarounds.
CSCed68879	On a Cisco router running Cisco IOS Release 12.1(15)BC1b with MC16S cards, the snmp returns a value for docsIfSigQSignalNoise that seems about 1000x higher than expected whereas CNR measurement on the interface shows that noise is in range. Workaround: For MC16S cards, use the CNR value from the **show interface cable** command line output rather than snmp response from docsIfSigQSignalNoise for problem determination. There are no known workarounds for MC16B and/or MC16C cards.

Table 30 Closed and Resolved Caveats for Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCed86358	A cable line card running IOS may crash. In some cases if the card does not have enough memory, it will crash to ROMMON and will not automatically reboot. This issue occurs under the following conditions: • HCCP must be configured on the linecard • Secondary service flows must be configured via the cable modem config file • A modem must have at one time been online and then gone offline and remain offline during an hccp switchover. The service flows for that modem are not de-allocated when it goes offline and are the source of the crash. • Performing a "show cable tech" or "show int CableX/Y/Z sid" after the switchover will access the sids that were not de-allocated and may crash either the card that has become Active or, if another switchover is done, the card that is Standby. There are no known workarounds other than to not configure secondary service flows if they are not truly needed.
CSCed87675	When it is indicated in the overrun register, IPM stuck is prematurely triggered. Also, punt packets per interface are accounted better. There are no known workarounds.
CSCee08163	The PRE may hang during an N+1 line card switchover with "cable source verify dhcp" enabled. It is caused due to a race condition in the code. There are no known workarounds.
CSCee11695	When the CMTS is configured with "cable source-verify dhcp", and bundling is configured, and ip pkts from CPE are being source verified, the lease query response may be incorrectly dropped; leading to the CMTS continuously sending lease query requests and dropping lease query acks. There are no known workarounds.
CSCee13327	Fib index may not be correctly set for the DHCP CPE's in pxf source-verify tables (affects mainly customers with MPLS VPN and source-verify dhcp configured). The output of "show pxf cable source-verify | i <sid>" will show a different Fib Index for CM and CPE or show multiple entries for the same IP address and SID but a different Fib index. Workaround: Do not configure "cable source-verify [dhcp]".
CSCee14029	Excessive source-verify punts to the RP. If this occurs on the uBR10012 router, it can render the router unusable temporarily. Workaround: Unconfigure source-verify.

Table 30 Closed and Resolved Caveats for Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCee20869	In order to protect from DOS service attacks on the CMTS, it was 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 no known workarounds.
CSCee21114	When "source-verify dhcp" and "no cable arp" are 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".
CSCee24107	The slot preference algorithm gives preference to PRE-A to become the active after a reload. This algorithm sometimes was not working, and PRE-B become the active on reload. Workaround: Do a PRE swtichover (redundancy force failover) if PRE-B became active.
CSCee27549	SNMP query does not detect specific modems via cdxCmCpeCmStatusIndex in new IOS code 12.2(15)BC1c code. This issue only occurs for few cable modems on uBR10012 router chassis. It is noticed that same cable modem, for which snmp poll is failing, appeared under multiple cable interfaces There are no known workarounds.
CSCee46682	The **show hardware pxf** command has been changed to the **show pxf** command in Cisco IOS Release 12.2(15)BC2 on uBR10012 router. This change needs to be added 12.2(15B)C1. There are no known workarounds.
CSCee70251	Given that the Network Access disabled, the CMTS would discard the following from a CM: • BPI Auth-Request • DSA/DSC/DSD This, in turn, causes the following: • The CM to be stuck in the online(d) state • DOCSIS 1.0+ VoIP failure There are no known workarounds.

Table 30 Closed and Resolved Caveats for Release 12.2(15)BC1d (continued)

Caveat ID Number	Description
CSCee76039	With Cisco IOS Release 12.2(15)BC2d images, encrypted multicast will not work. Workaround: Do not encrypt multicast traffic.
CSCin75900	The networks connected to the CPE router (in case of business customers) become unreachable after PRE switchover if "cable source-verify [dhcp]" is configured on the CMTS (sub)interface associated with the modem. There are no known workarounds.

Open Caveats for Release 12.2(15)BC1c

All the caveats listed in Table 37 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 31 Open Caveats for Cisco IOS Release 12.2(15)BC1c

Caveat ID Number	Description
CSCdx78723	Both Working & protect interfaces may become active for a short period if the Working line card is reset or OIRed. There are no known workarounds.

CSCdy76009	If a uBR10012 router cable line card is pulled, shutdown, or powered off, and the show controller is subsequently issued, the user sees "- Hardware is Removed" for the card when he should see (for example):
	`"Interface Cable7/0/1`
	`Hardware is UBR10000 CLC - Removed"`
	This incomplete output can be seen on any 12.2BC release through August 2003.
	There are no known workarounds, but the **show run | inc card** command will show all configured card types, which is similar in output.

CSCdz28737	When in the interface configuration mode:
	`conf t`
	`interface x/y`
	If the standby PRE is coming up and a configuration is entered on the primary PRE it will not be synched across to the secondary PRE.
	Workaround: Wait until the standby PRE is in Hot Standby before entering the interface configuration mode.
	Alternative workaround: Exit the interface configuration mode and re-enter. Then re-issue the configuration commands

CSCdz29957	The Last input param is only updated when a packet is punted for processing in the slow path. Last input param is not updated when packets are processed by the fast path. There are no known workarounds.

Table 31 Open Caveats for Cisco IOS Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCea08812	This problem shows up when running multicast over bundle interfaces. If a client leaves the multicast group the CMTS will continue to forward multicast traffic on that interface. This only causes a performance problem because unnecessary traffic is consuming the available bandwidth. There are no known workarounds.
CSCea41090	On a uBR10012 router running 12.2(11)CY or 12.2(11)BC3, configured with bundling, IGMP messages received on the upstream will be echoed back on all the downstreams of the cable bundle instead of only those that have previously received IGMP joins. There are no known workarounds.
CSCea41491	After a PRE switchover, the show cable modem vendor summary command may produce output inconsistent with the show cable modem summary command. There ar e no known workarounds.
CSCea80895	Reliability counter in 'show interface cable' decrease without error. Cisco IOS software version 12.2(11)CY. There are no known workarounds.
CSCea82892	“clear cable flap-list all save-counters” does not save the counters This issue is seen only in uBR10012 router. There are no known workarounds.
CSCeb26908	The available downstream bandwidth value is not consistent among different CLI commands. There are no known workarounds.
CSCeb48061	When we issue a clear cab modem etc.on the RP, an IPC is sent to the LCs. The LCs then mark the modems offline and send another IPC to the RP so that the RP can then mark the same modems offline. Customer would see messages like the following on RP. Modems and would lose connectivity and go offline.: `UTC: %UBR10K-6-CM_INCONSISTENCY: CM state inconsistency 0000.395f.2259(msgp 0000.395f.2259), sid 206 (206), mac state 16, hwidb Cable5/0/4` This issue can occur during maintenance or configuration when the CLI (cle cable modem) is followed by a switchover. There are no known workarounds.
CSCeb59073	N+1/BPI+ is not officially supported yet. There are no known workarounds.
CSCeb59781	When switchover the slave interface, the IGMP client on that interface may have multicast traffic lost. Workaround: Use “clear ip mroute *”

Table 31 Open Caveats for Cisco IOS Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCeb67903	If an MC520S card receives a ranging request that is reported to be more than 4096Hz away from the desired upstream frequency, the MC520S card will command the modem in question to change it's upstream frequency in the wrong direction causing the modem to fall offline. This problem typically only affects cable modems with extremely poor upstream frequency calibration just after they initially come online or just after changing upstream channel characteristics. In some cases such modems with poor upstream frequency calibration may work better using lower upstream frequencies and wider channel widths. There are no known workarounds.
CSCeb76602	Spurious memory access may happen during HCCP config/unconfig. Workaround: Shut the Protect interface(s) associated with this HCCP group, then configure HCCP before re-enabling HCCP.
CSCeb77578	When the cable line card is hot swapped or plugin during run time, the upstream trap is missing. Workaround. Do not depend on the trap. Check the upstream ifOperStatus for the state.
CSCeb78298	Spurious memory access is observed on RP after copying startup (with N+1 config) to running config. There are no known workarounds.
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. There are no known workarounds.

CSCec14598	The router does not transmit RADIUS packets to a RADIUS server when information regarding which radius server to use is downloaded via a protocol other than RADIUS.
	This issue only occurs 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:
	`<CmdBold>radius-server host`
	`<CmdArg>x.x.x.x<NoCmdArg><noCmdBold>`
	Where 'x.x.x.x' is an arbitrary ipv4 address.

CSCec30612	When a CM is reset either from the CMTS or the CM itself, if the CM is using a docsis 1.0 qos profile, the reset is not propagated from the CLC to the RP. There are no known workarounds.

Table 31 Open Caveats for Cisco IOS Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCec30869	If the first cable interface is admin shutdown, when show cable modem CLI is typed on the PRE, the title header associated with the CLI output is not shown. There are no known workarounds.
CSCec44859	If the failure case is Keepalive failure when configure N+1/MC520 on uBR10012 router, the DS0,1,2,3 interfaces automatically revert back to the working interface from the protect interface This issue occurs on Cisco IOS software version 12.2(15)BC1. There are no known workarounds.
CSCec47748	With a uBR10012 router connected to a 7200 (NPE-G1) gig interface, when you reload the 7200 the uBR10012 router will be able to ping the 7200, but the 7200 can not ping the uBR10012 router. Workaround: Reload the uBR10012 router.
CSCec48387	Gates at committed states for active voice call can be stuck after LC OIR. There are no known workarounds.
CSCin36219	The max cpe configurations are not synched to the Standby PRE. After a PRE switch-over, the max cpe configurations will be set to unlimited. There are no known workarounds.
CSCin36271	Cable filter groups are persistent through a PRE switch-over. Workaround: Reconfigure the cable filter groups after switch-over.
CSCin41164	If a packet has more than 60 bytes suppressed by PHS, CMTS fails to properly restore the packet. This bug does not affect JIB based line card such as MC520S, MC520U and TransAm. In the first 64 bytes of a packet, it contains two bytes IP checksum, and another two bytes for TCP or UDP checksum. So, it is not likely a problem in customer sites to have more than 60 bytes suppressed by PHS. There are no known workarounds.
CSCin46885	CMTS does not allow CM to register with DOCSIS1.1 configuration file with DMIC enabled scenario for the CM which is already marked. Workaround: Remove the marking by “clear cable modem ? lock” or “clear cable modem ? delete” at CMTS and make the CM to came operational with DOCSIS1.1 configuration file.
CSCin48221	When a rogue CM is displayed in show cable modem rogue, the spoof count is a negative number and a junk dynamic secret is being displayed when none was configured. There are no known workarounds.

Table 31 Open Caveats for Cisco IOS Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCin48325	This problem happens when a cable interface is configured as an HCCP protect. And then if a user configures the 1st sub-interface on the interface, the interface line state after configuration will stay down, and never comes as up, until a shut-no-shut is done, after which line protocol state comes up. This does not happen when adding a second or more sub-interfaces.
CSCin49976	The packets received counters of native vlans in the output of “show vlan” may shoot up to very high unexpected values after a “clear vlan statistics” is done. The problem is created by re-configuring an existing VLAN to act as the Native VLAN. The work around is to delete the existing VLAN first then add it back in as the Native VLAN. There are no known workarounds.
CSCin50638	Redundant CLI options shown under <show hardware?>. There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC1c

The caveats listed in Table 38 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 32 Closed and Resolved Caveats for Release 12.2(15)BC1c

Caveat ID Number	Description
CSCdz85628	Unable to get the MIB value “cdrqCmtsCmStatusTable” from another SNMP agent. Workaround: Display the remote-query info from the command line using **show cable modem remote-query** command on CMTS.
CSCec65787	show proc mem sorted may crash the router with a large number of modems. Workaround: Use show proc mem.
CSCec76205	A PRE switch-over to the Standby PRE fails with 34,000 modems on the uBR10012 router. The process takes 5 minutes and line cards reset and modems do not come online. Successful switch-overs have been performed with 10K-15K modems at other sites. It's unknown what the modem limit is. Workaround: Reset the Line-cards manually to bring modems back online.
CSCec83212	During modem registration the Active PRE will consume all IO memory when the modem count reaches 27K-29K. This problem is specific to 12.2(15)BC1a. There are no known workarounds.

Table 32 Closed and Resolved Caveats for Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCec87802	High cpu utilization mostly due to CEF Scanner. This issue is observed on a uBR10012 router series that is running IOS 12.2(15)BC1. There are no known workarounds.
CSCed02703	Background statistics collection called from the CEF process is consuming high CPU levels on the RP when the CMTS is in steady state. There are no known workarounds.
CSCed03064	SNMP ENGINE process CPU usage is triggered by external MIB objects query. As long as there are one or many network management system querying the CMTS for some MIB objects, the SNMP ENGINE process will consume some CPU usage as SNMP ENGINE process is normal priority process. Querying ifTable could cause high CPU spike. For example, getting the whole ifTable with get next command could cause high CPU spike above 30% in 35K CMs system with total CPU load around 75%. There are no known workarounds.
CSCed09930	A Cisco Universal Broadband Router may reload unexpectedly as a result of its memory getting corrupted. This issue occurs only when using the CMTS remote query feature. Workaround: Disable the remote query by no cable modem remote-query.
CSCed16691	PXF internal packet memory for a certain linecard may get stuck after a uBR10012 router boots up. This will cause all packets coming into that linecard to get dropped. When RP detects that PXF IPM is stuck by default it will print a PXF_DMA-3-FBB_LINE_CARD error message If packet drops are observed one can recover by executing the **microcode reload pxf** command. Automatic PXF reload can be configured using the **exception pxf ipm** command in the global configuration. There are no known workarounds.
CSCed17260	In VPN environment, when there are CMs/CPEs getting the same ip address in different subinterfaces, a newly added source-verify entry with the same ip address may overwrite the previous CMs/CPEs source-verify entries. This does not cause any connectivity problem, however, will cause performance and scalability issues. There are no known workarounds.
CSCed17487	If we have around 44K modems on a uBR10012 router, it may take up to 9 minutes for the PRE failover to complete. There are no known workarounds.

Table 32 Closed and Resolved Caveats for Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCed21438	The CMTS rewrites the IP source of the DHCP OFFER to the pc client and changes it to the PRIMARY subnet on the Cable interface which breaks ACL's that are installed in the CM DOCSIS config file. This is when running "cable dhcp-giaddr policy" where the relay-agent is smart enough to decide how to populate the giaddr with the correct subnet depending whether the BROADCAST is coming from a PC or cable modem. The CMTS is following the rule according to RFC 1542 with regards to the giaddr, yet the spec does NOT specify clear cut rules for the source IP address of the packet. Cisco implementation rewrites the IP Source to the cable modem subnet during the OFFER. This is not wrong but under certain conditions where security filters reside in the DOCSIS config file get broken. There are no known workarounds.
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.
CSCed31927	During a PRE switch-over, a IPC trace-back may be noticed with a high number of modems. There are no known workarounds.

Table 32 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.
CSCed45663	In a specific circumstance a cmts will crash due to a bus error when the **cable arp filter request-send** command is configured. Specifically, BPI or BPI+ must be enabled and there must be IP traffic to a destination with no arp entry from a BPI modem for the crash to occur. This IP traffic will force an arp request to be sent. The filter logic will crash when determining if the arp request should be sent or filtered. This crash will not occur if BPI is not configured on the chassis. Workaround: If BPI is configured, disable the **cable arp filter request-send** command. The **cable arp filter reply-accept** can still be used regardless of the BPI configuration.
CSCed55652	When CIR flows are being used in a uBR10012 router, certain race conditions that can occur while configuring queues may result in lowered performance for flows on affected downstreams. There are no known workarounds.
CSCed60220	A memory leak occurs in the *Dead* process on the PRE. Workaround: Disable AAA Exec Accounting and Network accounting.
CSCed68829	Some modems might not be queried from SNMP cdxCmCpeTable and linecard CLI “show cable device access-group”. Workaround: shut/no shut the cable interface.

Table 32 Closed and Resolved Caveats for Release 12.2(15)BC1c (continued)

Caveat ID Number	Description
CSCed72979	Cable Line Cards may become unresponsive under certain conditions. If this happens, the card will go offline, but it will not reboot itself. It has to be reset manually using the **hw-module reset** command. There are no known workarounds.

CSCed76837	If there are lots of CM/CPE in the linecard, the SNMP query MIB tables related the CM/CPE info will possibly have SNMP-3-CPUHOG message and trackback. Also the CM/CPE may have connection problem (drop offline or lose VPN).
	The MIB tables are listed below. They are all invoke the same API to get the sorted table which the entry is searched.
	`CISCO-DOCS-EXT-MIB:cdxCmCpeTable,`
	`DOCS-IF-MIB:docsIfCmtsMacToCmTable`
	`DOCS-QOS-MIB:docsQosCmtsMacToSrvFlowTable`
	`CISCO-DOCS-REMOTE-QUERY-MIB:cdrqCmtsCmStatusTable`
	After fix:
	– All the SNMP query for above tables will get info from RP/NPE only. So LC will not be affected.
	– The SNMP query Get EXACT will have real time response.
	– SNMP Get NEXT for above MIB tables is too expensive in a big system since it needs to go through whole CM/CPE in order to know which CM/CPE is the next entry of the query. Users are recommended to use SNMP GET EXACT to retrieve the info for a specific device.
	In order to prevent CPU spiking for GET NEXT for above MIB tables, In the CMTS which number of devices (CM/CPE) is greater than 1000, the SNMP query GET NEXT will not get any entries returned. GetBulk has also the same problem as GetNext since internally, it searches for the next entry.
	There are no known workarounds.

CSCee07031	Wrong cdxCmCpeCmStatusIndex value which does not matched the docsIfCmtsCmStatusIndex. MIB object affected by this problem: cdxCmCpeCmStatusIndex and docsIfCmtsCmPtr There are no known workarounds.

Open Caveats for Release 12.2(15)BC1b

All the caveats listed in Table 37 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 33 Open Caveats for Cisco IOS Release 12.2(15)BC1b

Caveat ID Number	Description
CSCdx78723	Both Working & protect interfaces may become active for a short period if the Working line card is reset or OIRed. There are no known workarounds.

CSCdy76009	If a uBR10012 router cable line card is pulled, shutdown, or powered off, and the show controller is subsequently issued, the user sees "- Hardware is Removed" for the card when he should see (for example):
	
	`"Interface Cable7/0/1`
	`Hardware is UBR10000 CLC - Removed"`
	
	This incomplete output can be seen on any 12.2BC release through August 2003.
	
	There are no known workarounds, but the **show run | inc card** command will show all configured card types, which is similar in output.

CSCdz28737	When in the interface configuration mode:
	
	`conf t`
	`interface x/y`
	
	If the standby PRE is coming up and a configuration is entered on the primary PRE it will not be synched across to the secondary PRE.
	
	Workaround: Wait until the standby PRE is in Hot Standby before entering the interface configuration mode.
	
	Alternative workaround: Exit the interface configuration mode and re-enter. Then re-issue the configuration commands.

CSCdz29957	The Last input param is only updated when a packet is punted for processing in the slow path. Last input param is not updated when packets are processed by the fast path. There are no known workarounds.
CSCdz85628	Unable to get the MIB value "cdrqCmtsCmStatusTable" from another SNMP agent. Workaround: Display the remote-query info from the command line using **show cable modem remote-query** command on CMTS.
CSCea08812	This problem shows up when running multicast over bundle interfaces. If a client leaves the multicast group the CMTS will continue to forward multicast traffic on that interface. This only causes a performance problem because unnecessary traffic is consuming the available bandwidth. There are no known workarounds.

Table 33 Open Caveats for Cisco IOS Release 12.2(15)BC1b (continued)

Caveat ID Number	Description
CSCea41090	On a uBR10012 router running 12.2(11)CY or 12.2(11)BC3, configured with bundling, IGMP messages received on the upstream will be echoed back on all the downstreams of the cable bundle instead of only those that have previously received IGMP joins. There are no known workarounds.
CSCea41491	After a PRE switchover, the show cable modem vendor summary command may produce output inconsistent with the show cable modem summary command. There are no known workarounds.
CSCea80895	Reliability counter in 'show interface cable' decrease without error. This problem occurs on Cisco IOS software version 12.2(11)CY. There are no known workarounds.
CSCea82892	“clear cable flap-list all save-counters” does not save the counters This problem is seen only in uBR10012 router. There are no known workarounds.
CSCeb26908	The available downstream bandwidth value is not consistent among different CLI commands. There are no known workarounds.
CSCeb48061	When we issue a clear cab modem etc.on the RP, an IPC is sent to the LCs. The LCs then mark the modems offline and send another IPC to the RP so that the RP can then mark the same modems offline. Customers would see messages like the following on RP and modems would lose connectivity and go offline: `UTC: %UBR10K-6-CM_INCONSISTENCY: CM state inconsistency 0000.395f.2259(msgp 0000.395f.2259), sid 206 (206), mac state 16, hwidb Cable5/0/4` It can occur during maintenance or configuration when the CLI (cle cable modem) is followed by a switchover There are no known workarounds.
CSCeb58851	The CMTS may display an error message, like the one below, when a **hw-module reset** command is issued: `SLOT 8/1: Jul  8 15:31:25.283: %SYS-3-CPUHOG: Task ran for 2104 msec (3/3), proc ess = CR10K CLC Delete all SIDs task, PC = 604258D4.` This may happen when several interfaces are down at the same time and there are a lot of modems attached to those interfaces.
CSCeb59073	N+1/BPI+ is not officially supported yet. There are no known workarounds.

Table 33 Open Caveats for Cisco IOS Release 12.2(15)BC1b (continued)

Caveat ID Number	Description
CSCeb59781	When switchover the slave interface, the IGMP client on that interface may have multicast traffic lost. Workaround: Use “clear ip mroute *”
CSCeb67903	If an MC520S card receives a ranging request that is reported to be more than 4096Hz away from the desired upstream frequency, the MC520S card will command the modem in question to change it's upstream frequency in the wrong direction causing the modem to fall offline. This problem typically only affects cable modems with extremely poor upstream frequency calibration just after they initially come online or just after changing upstream channel characteristics. In some cases such modems with poor upstream frequency calibration may work better using lower upstream frequencies and wider channel widths. There are no known workarounds.
CSCeb76602	Spurious memory access may happen during HCCP config/unconfig. Workaround: Shut the Protect interface(s) associated with this HCCP group, then configure HCCP before re-enabling HCCP.
CSCeb77578	When the cable line card is hot swapped or plugin during run time, the upstream trap is missing. Workaround: Do not depend on the trap. Check the upstream ifOperStatus for the state.
CSCeb78298	Spurious memory access is observed on RP after copying startup (with N+1 config) to running config There are no known workarounds.
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. There are no known workarounds.

CSCec14598	The router does not transmit RADIUS packets to a RADIUS server when information regarding which radius server to use is downloaded via a protocol other than RADIUS.
	This issue only occurs 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:
	`<CmdBold>radius-server host`
	`<CmdArg>x.x.x.x<NoCmdArg><noCmdBold>`
	Where 'x.x.x.x' is an arbitrary ipv4 address.

Table 33 Open Caveats for Cisco IOS Release 12.2(15)BC1b (continued)

Caveat ID Number	Description
CSCec30612	When a CM is reset either from the CMTS or the CM itself, if the CM is using a docsis 1.0 qos profile, the reset is not propagated from the CLC to the RP. There are no known workarounds.
CSCec30869	If the first cable interface is admin shutdown, when show cable modem CLI is typed on the PRE, the title header associated with the CLI output is not shown. There are no known workarounds.
CSCec44859	If the failure case is Keepalive failure when configure N+1/MC520 on uBR10012 router, the DS0,1,2,3 interfaces automatically revert back to the working interface from the protect interface This problem occurs in Cisco IOS software version 12.2(15)BC1. There are no known workarounds.
CSCec47748	With a uBR10012 router connected to a 7200 (NPE-G1) gig interface, when you reload the 7200 the uBR10012 router will be able to ping the 7200, but the 7200 can not ping the uBR10012 router. Workaround: Reload the uBR10012 router.
CSCec48387	Gates at committed states for active voice call can be stuck after LC OIR. There are no known workarounds.
CSCin36219	The max cpe configurations are not synched to the Standby PRE. After a PRE switch-over, the max cpe configurations will be set to unlimited. There are no known workarounds.
CSCin36271	Cable filter groups are persistent through a PRE switch-over. Workaround: Reconfigure the cable filter groups after switch-over.
CSCin41164	If a packet has more than 60 bytes suppressed by PHS, CMTS fails to properly restore the packet. This bug does not affect JIB based line card such as MC520S, MC520U and TransAm. In the first 64 bytes of a packet, it contains two bytes IP checksum, and another two bytes for TCP or UDP checksum. So, it is not likely a problem in customer sites to have more than 60 bytes suppressed by PHS. There are no known workarounds.
CSCin46885	CMTS does not allow CM to register with DOCSIS1.1 configuration file with DMIC enabled scenario for the CM which is already marked. Workaround: Remove the marking by “clear cable modem ? lock” or “clear cable modem ? delete” at CMTS and make the CM to came operational with DOCSIS1.1 configuration file.
CSCin48221	When a rogue CM is displayed in show cable modem rogue, the spoof count is a negative number and a junk dynamic secret is being displayed when none was configured. There are no known workarounds.

Table 33 Open Caveats for Cisco IOS Release 12.2(15)BC1b (continued)

Caveat ID Number	Description
CSCin48325	This problem happens when a cable interface is configured as an HCCP protect. And then if a user configures the 1st sub-interface on the interface, the interface line state after configuration will stay down, and never comes as up, until a shut-no-shut is done, after which line protocol state comes up. This doesn't happen for adding 2nd and more sub-interfaces. There are no known workarounds.
CSCin49976	The packets received counters of native vlans in the output of “show vlan” may shoot up to very high unexpected values after a “clear vlan statistics” is done. The problem is created by re-configuring an existing VLAN to act as the Native VLAN. The work around is to delete the existing VLAN first then add it back in as the Native VLAN. There are no known workarounds.
CSCin50638	Redundant CLI options shown under <show hardware?> There are no known workarounds.

Closed and Resolved Caveats for Release 12.2(15)BC1b

The caveats listed in Table 38 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 34 Closed and Resolved Caveats for Release 12.2(15)BC1b

Caveat ID Number	Description
CSCeb4012	Maximum DS throughput much below 10MB was observed for business subscribers with MIR configuration of 10Mbps because of tail drops in PXF queues. The packet drops will cause the TCP sessions to throttle back and so the throughput for these sessions will be lower than the MIR configured for the flow. This problem affects TCP sessions with high bandwidth downstream flows. There are no known workarounds.
CSCeb76582	This fix ensures that the new tables defined in PXF for the VTMS mir fix CSCeb37891 are correctly initialized to zero. There are no known workarounds.
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.

Table 34 Closed and Resolved Caveats for Release 12.2(15)BC1b (continued)

Caveat ID Number	Description
CSCec19196	Some CPE's may loose IP connectivity after installing IOS 12.2(15)BC1 on an uBR10012 router router. This problem occurs when a cable subinterface is configured for **cable-source-verify [dhcp]**. Workaround: Remove **cable source-verify [dhcp]** on the cable subinterface or entering **clear cable modem <mac> delete** for affected Cable Modems restores IP connectivity.
CSCec45384	When using 20ms packetization rate, some of the calls made are dropping packets. This happens with some MTAs. There are no known workarounds.
CSCec47470	A uBR10012 router may crash with an error message similar to %ALIGN-1-FATAL: Illegal access to a low address. There are no known workarounds.
CSCec51242	If an invalid gate id is specified in the show packetcable gate command, it can cause a crash at random due to invalid memory access. There are no known workarounds.
CSCec54694	After several weeks of uptime, cable modem traffic is not being correctly routed to the DHCP server configured as helper-address. This problem occurs when tag-switching (MPLS) is enabled on the backhaul GigE interface. Workaround: Use clear ip route <address of DHCP Server>
CSCec55868	On the uBR10012 router, it is possible that high priority traffic can be dropped on the 5x20 linecard because the back pressure mechanism to throttle PXF is not working. This is only a problem during link congestion. There are no known workarounds.
CSCec56459	In VPN setting, when do "show hard pxf cable source-verify", there are zero empty entries shown. It does not affect the functionality of cable source-verify. There are no known workarounds.
CSCec61676	When cable intercept is enabled, those intercepted packets show to have extra bytes appended and this causes replay problem on CALEA server. There are no known workarounds.
CSCec85777	This bug is used to release a new 5x20 MAC chip firmware version. There are no known workarounds.
CSCec85800	This bug was filed to release certain debugging capabilities in the PXF. There are no known workarounds.
CSCec89558	MC5x20 line-card to line-card communication may fail. There are no known workarounds.

Table 34 Closed and Resolved Caveats for Release 12.2(15)BC1b (continued)

Caveat ID Number	Description
CSCed03085	On a uBR10012 router, when a CPE is disconnected and the corresponding ARP entry times out, some internal structures may not be reclaimed until the mac rewrite index pool is depleted and indices are reclaimed and reused. As a result, the DHCPD process can show up as holding a large amount of memory (in the order of 10 MB). Workaround: shut/no shut the cable interfaces.
CSCed07613	If a gate-delete message is received from CMS, the gate state and service flow on the RP are cleaned up, but corresponding toaster resources may not be cleaned up. If several such gate-delete messages are received, it may eventually exhaust toaster resources, resulting in QALLOC failures. There are no known workarounds.
CSCed12910	During continuous operation of the uBR10012 router, it is possible that an odd numbered downstream on the 5x20 linecard gets stuck, causing all the CMs to go offline. The corresponding even numbered downstream, will lose IP connectivity as a result. As a result on the even numbered downstream CMs that try to reregister will get stuck in init(i) state. To recover from the problem, you need to reload the linecard. There are no known workarounds.
CSCin54155	The uBR10012 router uses internal access-lists for various functions that do not appear in the running configuration but are displayed in the 'show access-list' output for debugging purposes. These access-lists are prefixed with 'CMTS_PKT_FILTER_GROUP'. If these access lists are removed using the global configuration CLI, it can cause router malfunction including a crash. Workaround: Do not disable these internal access-lists.

Open Caveats for Release 12.2(15)BC1a

All the caveats listed in Table 37 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 35 Open Caveats for Cisco IOS Release 12.2(15)BC1a

Caveat ID Number	Description
CSCdx78723	Both Working & protect interfaces may become active for a short period if the Working line card is reset or OIRed. There are no known workarounds.

CSCdy76009	If a uBR10012 router cable line card is pulled, shutdown, or powered off, and the show controller is subsequently issued, the user sees "- Hardware is Removed" for the card when he should see (for example):
	`"Interface Cable7/0/1`
	`Hardware is UBR10000 CLC - Removed"`
	This incomplete output can be seen on any 12.2BC release through August 2003.
	There are no known workarounds, but the **show run | inc card** command will show all configured card types, which is similar in output.

CSCdz28737	When in the interface configuration mode:
	`conf t`
	`interface x/y`
	If the standby PRE is coming up and a configuration is entered on the primary PRE it will not be synched across to the secondary PRE.
	Workaround: Wait until the standby PRE is in Hot Standby before entering the interface configuration mode.
	Alternative Workaround: Exit the interface configuration mode and re-enter. Then re-issue the configuration commands.

CSCdz29957	The Last input param is only updated when a packet is punted for processing in the slow path. Last input param is not updated when packets are processed by the fast path. There are no known workarounds.
CSCdz85628	Unable to get the MIB value "cdrqCmtsCmStatusTable" from another SNMP agent. Workaround: Display the remote-query info from the command line using **show cable modem remote-query** command on CMTS.
CSCea08812	This problem shows up when running multicast over bundle interfaces. If a client leaves the multicast group the CMTS will continue to forward multicast traffic on that interface. This only causes a performance problem because unnecessary traffic is consuming the available bandwidth. There are no known workarounds.

Table 35 Open Caveats for Cisco IOS Release 12.2(15)BC1a (continued)

Caveat ID Number	Description
CSCea41090	On a uBR10012 router running 12.2(11)CY or 12.2(11)BC3, configured with bundling, IGMP messages received on the upstream will be echoed back on all the downstreams of the cable bundle instead of only those that have previously received IGMP joins. There are no known workarounds.
CSCea41491	After a PRE switchover, the **show cable modem vendor summary** command may produce output inconsistent with the **show cable modem summary** command. There are no known workarounds.
CSCea80895	The reliability counter in "show interface cable" decreases without error. This occurs on Cisco IOS software version 12.2(11)CY There are no known workarounds.
CSCea82892	The "clear cable flap-list all save-counters" doesn't save the counters. This problem is seen only in uBR10012 router. There are no known workarounds.
CSCeb21333	Primary PRE stops sync' ing config commands to Secondary PRE. Workaround: To get synchronization to work again, hit <Enter> key a few times on secondary PRE console. Console response time is very slow since it keeps trying to sync to secondary.
CSCeb26908	The available downstream bandwidth value is not consistent among different CLI commands. There are no known workarounds.
CSCeb40129	Maximum DS throughput much below 10MB was observed for business subscribers with MIR configuration of 10Mbps because of tail drops in PXF queues. The packet drops will cause the TCP sessions to throttle back and so the throughput for these sessions will be lower than the MIR configured for the flow. This problem affects TCP sessions with high bandwidth downstream flows. There are no known workarounds.
CSCeb48061	When a clear cab modem etc. is issued on the RP, an IPC is sent to the LCs. The LCs then mark the modems offline and send another IPC to the RP so that the RP can then mark the same modems offline. The following messages will appear: `UTC: %UBR10K-6-CM_INCONSISTENCY: CM state inconsistency 0000.395f.2259(msgp 0000.395f.2259), sid 206 (206), mac state 16, hwidb Cable5/0/4` On RP, modems would lose connectivity and go offline. It can occur during maintenance or configuration when the CLI (cle cable modem) is followed by a switchover There are no known workarounds.

Table 35 Open Caveats for Cisco IOS Release 12.2(15)BC1a (continued)

Caveat ID Number	Description
CSCeb58851	The CMTS may display the following error message when a **hw-module reset** command is issued: `SLOT 8/1: Jul  8 15:31:25.283: %SYS-3-CPUHOG: Task ran for 2104 msec (3/3), proc ess = CR10K CLC Delete all SIDs task, PC = 604258D4.` This may happen when several interfaces are down at the same time and there are a lot of modems attached to those interfaces. There are no known workarounds.
CSCeb59073	N+1/BPI+ is not officially supported yet. There are no known workarounds.
CSCeb59781	When switchover the slave interface, the IGMP client on that interface may have multicast traffic lost. Workaround: Use “clear ip mroute *”
CSCeb67903	If an MC520S card receives a ranging request that is reported to be more than 4096Hz away from the desired upstream frequency, the MC520S card will command the modem in question to change it's upstream frequency in the wrong direction causing the modem to fall offline. This problem typically only affects cable modems with extremely poor upstream frequency calibration just after they initially come online or just after changing upstream channel characteristics. In some cases such modems with poor upstream frequency calibration may work better using lower upstream frequencies and wider channel widths. There are no known workarounds.
CSCeb76602	Spurious memory access may happen during HCCP config/unconfig. Workaround: Shut the Protect interface(s) associated with this HCCP group, then configure HCCP before re-enabling HCCP.
CSCeb77578	When the cable line card is hot swapped or plugin during run time, the upstream trap is missing. Workaround. Do not depend on the trap. Check the upstream ifOperStatus for the state.
CSCeb78298	Spurious memory access is observed on RP after copying startup (with N+1 config) to running config. There are no known workarounds.
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. There are no known workarounds.

Table 35 Open Caveats for Cisco IOS Release 12.2(15)BC1a (continued)

Caveat ID Number	Description

CSCec14598	The router does not transmit RADIUS packets to a RADIUS server when information regarding which radius server to use is downloaded via a protocol other than RADIUS.
	This issue only occurs 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:
	`<CmdBold>radius-server host`
	`<CmdArg>x.x.x.x<NoCmdArg><noCmdBold>`
	Where 'x.x.x.x' is an arbitrary ipv4 address.

CSCec19196	Some CPE's may loose IP connectivity after installing IOS 12.2(15)BC1 on an uBR10012 router router. A cable subinterface is configured for **cable-source-verify [dhcp]**. Workaround: Remove **cable source-verify [dhcp]** on the cable subinterface Alternative Workaround: Entering **clear cable modem <mac> delete** for affected Cable Modems will restore IP connectivity.
CSCec30612	When a CM is reset either from the CMTS or the CM itself, if the CM is using a docsis 1.0 qos profile, the reset is not propagated from the CLC to the RP. There are no known workarounds.
CSCec30869	If the first cable interface is admin shutdown, when show cable modem CLI is typed on the PRE, the title header associated with the CLI output is not shown. There are no known workarounds.
CSCec44859	If the failure case is Keepalive failure when configure N+1/MC520 on uBR10012 router, the DS0,1,2,3 interfaces automatically revert back to the working interface from the protect interface. This occurs on Cisco IOS software version 12.2(15)BC1. There are no known workarounds.
CSCec47470	A uBR10012 router may crash with an error message similar to the following: `%ALIGN-1-FATAL: Illegal access to a low address` There are no known workarounds.
CSCec47748	With a uBR10012 router connected to a 7200 (NPE-G1) gig interface, when you reload the 7200 the uBR10012 router will be able to ping the 7200, but the 7200 can not ping the uBR10012 router. Workaround: Reload the uBR10012 router.
CSCec48387	Gates at committed states for active voice call can be stuck after LC OIR. There are no known workarounds.

Table 35 Open Caveats for Cisco IOS Release 12.2(15)BC1a (continued)

Caveat ID Number	Description
CSCec56459	In VPN setting, when do “show pxf cable source-verify”, there are zero empty entries shown. It does not affect the functionality of cable source-verify. There are no known workarounds.
CSCin36219	The max cpe configurations are not synched to the Standby PRE. After a PRE switch-over, the max cpe configurations will be set to unlimited. There are no known workarounds.
CSCin36271	Cable filter groups are persistent through a PRE switch-over. Workaround: Reconfigure the cable filter groups after switch-over.
CSCin41164	If a packet has more than 60 bytes suppressed by PHS, CMTS fails to properly restore the packet. This bug does not affect JIB based line card such as MC520S, MC520U and TransAm. In the first 64 bytes of a packet, it contains two bytes IP checksum, and another two bytes for TCP or UDP checksum. So, it is not likely a problem in customer sites to have more than 60 bytes suppressed by PHS. There are no known workarounds.
CSCin46885	CMTS does not allow CM to register with DOCSIS1.1 configuration file with DMIC enabled scenario for the CM which is already marked. Workaround: Please remove the marking by “clear cable modem ? lock” or “clear cable modem ? delete” at CMTS and make the CM to came operational with DOCSIS1.1 configuration file.
CSCin48221	When a rogue CM is displayed in show cable modem rogue, the spoof count is a negative number and a junk dynamic secret is being displayed when none was configured. There are no known workarounds.
CSCin48325	This problem happens when a cable interface is configured as an HCCP protect. And then if a user configures the 1st sub-interface on the interface. The interface line state after configuration will stay down, and never comes as up, until a shut-no-shut is done, after which line protocol state comes up. This doesn't happen for adding 2nd and more sub-interfaces. There are no known workarounds.
CSCin49976	The packets received counters of native vlans in the output of “show vlan” may shoot up to very high unexpected values after a “clear vlan statistics” is done. The problem is created by re-configuring an existing VLAN to act as the Native VLAN. Workaround: Delete the existing VLAN first then add it back in as the Native VLAN.

Table 35 Open Caveats for Cisco IOS Release 12.2(15)BC1a (continued)

Caveat ID Number	Description
CSCin50638	Redundant CLI options shown under <show hardware?>. There are no known workarounds.
CSCin54155	The uBR10012 router uses internal access-lists for various functions that do not appear in the running configuration but are displayed in the "show access-list" output for debugging purposes. These access-lists are prefixed with "CMTS_PKT_FILTER_GROUP". If these access lists are removed using the global configuration CLI, it can cause router malfunction including a crash. Workaround: Don't disable these internal access-lists.

Closed and Resolved Caveats for Release 12.2(15)BC1a

The caveats listed in Table 38 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 36 Closed and Resolved Caveats for Release 12.2(15)BC1a

Caveat ID Number	Description
CSCeb62481	When PXF microcode crashes, PXF client writes a crashinfo onto bootflash: for future debugging purposes. In some cases "Tag debug data" in crashinfo could be useless. This issue is only a issue related to debuggability of a pxf crash. And doesn't affect router operation or any PXF functionality, as such. There are no known workarounds.
CSCec17473	After abnormal traffic pattern on cable interface, the "CR10K Request di" process increased by ~54 MB in "show proc cpu". Determined that buffers that overflow receive ring for process, were never freed. Workaround: Event does not appear frequent, only 1 incident in 22 weeks of uptime. However there is no known workaround to recover lost memory. System continued to run without incident following one time event.
CSCec22551	Packets from high bandwidth multicast streams can be dropped in the uBR10012 router when it is operating in the best-effort flow aggregation mode. There are no known workarounds.
CSCec26556	When configure cable qos enforce-rule without no-persistence, the enforced QoS profile does not work correctly in force when a cable modem reboot. Looks good regarding **show cable modem xxxx qos** command, but in fact, the traffic go through higher than MaxSusRate of enforced QoS profile. This occurs on a Cisco IOS software version 12.2(15)BC1 "cable qos enforce-rule" is configured. There are no known workarounds.

Table 36 Closed and Resolved Caveats for Release 12.2(15)BC1a (continued)

Caveat ID Number	Description

CSCec35575	Cisco Ubr10000 Cable linecard may crash in rare occasions with the following messages:
	`SLOT 5/1: 00:00:34: %UBR10000-5-UPDOWN: Interface Cable5/1/4 Port U0, changed state to administratively down`
	`SLOT 5/1: 00:00:34: %UBR10000-5-UPDOWN: Interface Cable5/1/4 Port U1, changed state to administratively down`
	`SLOT 5/1: 00:00:34: %UBR10000-5-UPDOWN: Interface Cable5/1/4 Port U2, changed state to administratively down`
	`SLOT 5/1: 00:00:34: %UBR10000-5-UPDOWN: Interface Cable5/1/4 Port U3, changed state to administratively downCMD: 'end' 08:31:19 UTC Wed Sep 17 2003`
	`%ALIGN-1-FATAL: Illegal access to a low address addr=0x1C, pc=0x6041F320, ra=0x6041EFC8, sp=0x6129C6B8`
	`%ALIGN-1-FATAL: Illegal access to a low address addr=0x1C, pc=0x6041F320, ra=0x6041EFC8, sp=0x6129C6B8`
	`Unexpected exception, CPU signal 10, PC = 0x6041F320`
	`-Traceback= 6041F320 6041C288`
	`$0 : 00000000, AT : 0300FE00, v0 : 00000000, v1 : 00000000`
	`a0 : 619489BC, a1 : 61944BF4, a2 : 00000000, a3 : 00000051`
	`t0 : 00000400, t1 : 3E800010, t2 : 00000001, t3 : 00000008`
	`t4 : 3400F900, t5 : 00000000, t6 : 00000000, t7 : 00008000`
	`s0 : 00000000, s1 : 00000000, s2 : 00000000, s3 : 61250C40`
	`s4 : 607A0000, s5 : 00000000, s6 : 61942B18, s7 : 607A0000`
	`t8 : 0D0D0D0D, t9 : 00000004, k0 : 00000000, k1 : 00000000`
	`gp : 60E24AA0, sp : 6129C6B8, s8 : 60F30000, ra : 6041EFC8`
	`EPC : 6041F320, ErrorEPC : FFFFFFFF, SREG : 3400F903`
	`MDLO : 22E0C319, MDHI : FE541066, BadVaddr : 0000001C`
	`Cause 0000000C (Code 0x3): TLB (store) exception`
	There are no known workarounds.

CSCec36157	Downstream QOS for service flows can be affected after a PXF reload. Workaround: Execute **clear cable modem all reset**

Table 36 Closed and Resolved Caveats for Release 12.2(15)BC1a (continued)

Caveat ID Number	Description
CSCec39936	New PXF microcode is being released with this bug report. It includes fixes for CSCec20324 & CSCec32351.
CSCin46501	Ping from CPE to CMTS fails under certain conditions, when source verify is configured. Ping from CPE to CMTS fails under the following scenario. 1. Create a sub-interface over a bundled interface 2. Configure “cable source-verify” on the new subinterface and assign primary and secondary address pools 3. Bring up a CPE using DHCP on the subinterface 4. Now change the CPE from DHCP-assigned address to static IP address from the secondary pool. Ping from CPE to CMTS fails. Workaround: Remove “cable source-verify” from the subinterface above.

Open Caveats for Release 12.2(15)BC1

All the caveats listed in Table 37 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 37 Open Caveats for Cisco IOS Release 12.2(15)BC1

Caveat ID Number	Description
CSCdw46656	None-shared version of Downstream Frequency Override broken in 10K
CSCdw92201	Schooner: No entAliasMappingEntry for PRE1 NetworkManagementEthernet
CSCdx59958	Multi-cast fails for the CPE connected behind the slave interface
CSCdx78723	Both Working & Protect interfaces are UP with the same IP Address
CSCdy28153	MC520S:Tracebacks observed after hw-module subslot reset
CSCdz15526	Optimization in shutting subinterface
CSCdz19043	cable privacy hotlist for manuf and cm cert not working
CSCdz28737	PRE-HA: Some CLIs configured on active PRE not reflected on secondary
CSCdz29957	Clipper: Last input not updated for pos int. with smartbits traffic
CSCdz49594	BPI Multicast not working with Bundling w/subif
CSCdz79038	PXF DMA FTC Bad Address Error with 12.2(11)CY
CSCdz85628	uBR10k:Unable to get the MIB value cdrqCmtsCmStatusTable
CSCdz85788	PXF DMA TBB Length Error with 12.2(11)CY
CSCea08812	CMTS keeps sending traffic on bundle intf. without m-cast members
CSCea31567	Inconsistencies in VRF arp table
CSCea41090	IGMP message should not be echoed to all interfaces in bundle
CSCea41491	sh cable modem vendor summary - shows wrong results

Table 37 Open Caveats for Cisco IOS Release 12.2(15)BC1 (continued)

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
CSCin54155	Deleting internal ACL followed by show access causes RP to crash
CSCin54216	CMTS crashed at strcmp,add_turboacl_in_list during copy from bootfla

Closed and Resolved Caveats for Release 12.2(15)BC1

The caveats listed in Table 38 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 38 Closed and Resolved Caveats for Release 12.2(15)BC1

Caveat ID Number	Description
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.
CSCdz23695	CPE database not updated with static IP address of new CPE until ARP
CSCdz46435	Traceback at frame_relay_extract_addr after igmp_get_mac_or_ip_srcad
CSCdz51438	Sch_p2:LC crashes after shut/no-shut us & clear cab modem all reset
CSCdz64816	<clear cable modem> syntax change
CSCdz68844	uBR10k:Blank system messages in logs and on syslog server
CSCdz71127	corrupted packet can cause input queue wedge - reg to CSCdx02283
CSCdz76022	uBR10k:sh int cable modem outputs incorrectly method.
CSCdz79703	SSO should failover if CEF gets disabled
CSCea02355	rare ip packets may cause input queue wedge
CSCea05168	UBR10k does not update mcast counters correctly while process switch
CSCea12543	MC520:power-level CLI does not work for 3.2MHz below -4 dbmv
CSCea22226	show cable hop runs Corr/Uncorr FEC counters together
CSCea25341	N+1/10k:Cannot show CNR per modem after switch-over

Table 38 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.
CSCea33742	MC520:modem fail to come online on unspecified upstream port
CSCea40614	Unable to disable parser error while coping start-up config to run
CSCea41322	CPUHOG error or bug error during switch over.
CSCea45202	DOCSIS:UCC is broken in DOCSIS1.1 mode
CSCea46180	UBR10K:mcast packets drop when join grp is defined in cable interface
CSCea46256	LC-HA:PXF incorrectly initialized for sub-interfaces
CSCea50802	Do not divert packets to PRE when modem online(d)
CSCea53519	PRE-HA: cable src-verify command not synced to secn pre after n+1 swi
CSCea54735	LC-HA: ip access-group <n> out CLI not synched across to Protect
CSCea57059	Add separate CLI to display different queue types
CSCea57487	LC-HA:IP address not synced to Standby PRE after N+1 switchover
CSCea61183	MC520S:Upstream down when spectrum group configured on upstream
CSCea63996	LC-HA: Protect interfaces may not go to Standby mode
CSCea65629	PRE-HA: Running config is executed twice on the Standby PRE
CSCea65880	UBR10K-6-CM_INCONSISTENCY msg and modem does not come up
CSCea69629	LC-HA: Line card crash after shut/no shut.
CSCea76756	ubr10k hang when source-verify dhcp and relay info opt configured
CSCea77176	Some MC520 cards not recognized with latest Flo_t image
CSCea77196	High CPU Utilization when unreachable packets come in SRP interface
CSCea82308	hide atp command due to being obsolete and causing traceback
CSCea83499	P2P app occasional small pkts dropped with MC520S in Downstream
CSCea83586	Downstream Sid Counters Increment Even If The Modems Are Offline
CSCea84297	cable qos profile [x] tos-overwrite AND OR requires CM re-register
CSCea87906	Spurious memory access made at 0x608E78D8 reading 0x0
CSCea90050	N+1/MC520S:US stuck on switchover - US PHY locks up
CSCea91498	Disable ATDMA CLIs
CSCeb00422	LC-HA:CPU Hog during switch-over with a large # of sub-interfaces
CSCeb00560	PRE crash at cmts_remove_bundle_entry & cmts_dhcp_glean

Table 38 Closed and Resolved Caveats for Release 12.2(15)BC1 (continued)

Caveat ID Number	Description
CSCeb00788	<clear cab modem delete> need to block IPC for layer 3
CSCeb03134	PRE-HA: configs not reflected on the standby PRE after lc switch
CSCeb05516	Line card may not recover after a crashing
CSCeb05570	PRE-HA - CPU Hog error at process = CR10K Request dispatcher
CSCeb11980	SUBMON: Make penalty qos profile enforcement persistence toggelable
CSCeb13104	IPC errors after overnight test - IPC message header cache is empty
CSCeb13563	5x20:CMTS crash observed after show cr10k cablex/x/x que cir
CSCeb16059	URB10K/VI: Snmpwalk - infinite loop at ifStackTable with VI
CSCeb18023	Traceback observed while applying service-policy to FastEthernet i/f
CSCeb22150	PXF drops pkts int ToRP q - buffer depletion under high load
CSCeb23929	PRE-HA: Shared/non-shared spectrum takes modems offline on RP
CSCeb24403	MC520:Illegal map after a UCD causes TI phy to lock up
CSCeb34775	%ALIGN-3-SPURIOUS traceback at pktcbl_cops_notify during bulk call
CSCeb38825	LC-HA: After switchover, Col2 MRI-Classif Table incorrect
CSCeb41300	10K:US overlap in shared mode, modems not online when changed CW
CSCeb44456	UBR10K - cable tftp-enforce mark-only flag wrongly CM
CSCeb45392	Add protection for a NULL pointer in cmts_bind_cm_to_upstream
CSCeb45601	PRE-HA: Pre switchover causes Protect cards to non-functional state
CSCeb50730	Mcast packets not all forwarded on MC520S
CSCeb51215	Crash from access to freed sh_mdb in c10k_mdfs_rp_update_stats
CSCeb51881	UBR10K:SNMP CPUHOG messages when line card is in down state
CSCeb52496	LC-HA:US overlap in spectrum management shared environment
CSCeb53299	LC-HA: Put in debug and workaround for CSCea63958 (MRI ASSERT crash)
CSCeb55392	LC-HA:PRE crash during LC switch-over; spectrum management related
CSCeb58199	LC-HA: Line card crash during switch over, with spectrum management
CSCeb58771	fair_enqueue called from process without int protection
CSCeb59552	Modems stay online and pingable with upstream freq Unassigned
CSCeb59760	10k/16S:Upstreams are still down after no shut
CSCeb59860	Should display NA for not support cli PHS counter.
CSCeb60153	LC-HA:PRE crash during switch-over when PRE CPU is above 90%
CSCeb64070	Potential crash in tbb_send_IPC_message after malloc failure
CSCeb68955	Fix for CSCea60819 (PRE crash on N+1 sw...) lost due to sync damage
CSCeb71752	PRE crash in sch_rp_setup_cable_queue()
CSCeb73026	LC-HA:HCCP_ASSERT message after switch-over.
CSCeb75194	LC-HA: Fast Fault Detection fails permanently after 1st trigger

Table 38 Closed and Resolved Caveats for Release 12.2(15)BC1 (continued)

Caveat ID Number	Description
CSCeb77720	When DMIC is enabled modems stuck at init(o) for >1600 byte conf fil
CSCeb78345	Initial maintenance slots not created under some circumstances
CSCeb85608	DS Mcast Pkt CRC error when mcast echo is enabled
CSCec00765	10k/16S:Upstream hops to the same frequency
CSCec00865	10k/16S:ACK39 after CMTS runs for 5 days
CSCec01544	GigE bouncing after access-list applied and removed
CSCin26768	LC-HA: Traffic matches wrong cfr on switchover followed by DSC
CSCin29305	PRE-HA: Traceback and MCASTECHO: Fail to obtain vcci for hwidb:
CSCin29836	UBR10K:ccsFlapLastClearTime reads 00 00s after clear cable flap all
CSCin37048	PRE-HA: Packets are not forwarding through secondary Dn SF after swit
CSCin37063	ip helper-address not removed when cable bundle <non-existent-bundle
CSCin37549	Traceback and Spurious memory access made at cmts_propagate_ip_confi
CSCin44163	Ambiguous command: for cli cable upstream 0 minislot-size 1
CSCin45098	Incoming PHS pkts after UCC are counted as InputErrors by CMTS
CSCin48353	cable shared-secret functionality is not working with ubr10000 image
CSCin48383	QoS profile in use can be made not-in-service
CSCin49248	PRE-HA: Standby crash by removing HCCP configs, then PRE switch-over
CSCin49445	MC520U:UBR crashed when docsQosServiceFlowStatsTable was queried
CSCin49468	LC-HA:CPE connectivity failed under N+1 switch over with source-veri
CSCin49570	Spurious memory access observed at cable_exec_command after qos enfo

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 39 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 39 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 40, 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 41.

Closed and Resolved Caveats for Release 12.2(11)BC3c

The caveats listed in Table 40 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 40 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 41 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 41 Open Caveats for Cisco IOS Release 12.2(11)BC3b

Caveat ID Number	Description
CSCdw46656	None-shared version of Downstream Frequency Override broken in 10K
CSCdz79038	PXF DMA FTC Bad Address Error with 12.2(11)CY
CSCdz85628	uBR10k: Unable to get the MIB value cdrqCmtsCmStatusTable
CSCea31567	Inconsistencies in VRF arp table
CSCea41090	IGMP message should not be echoed to all interfaces in bundle
CSCea42352	Setting HUGE buffer to greater than 65535 takes all CLC offline
CSCea83499	P2P app occasional small pkts dropped with MC520S in Downstream
CSCea93194	CMTS: Incorrect GigE output rate counter
CSCeb03001	DHCP forwarding performance is slow
CSCeb04474	5x20:Modems went offline with %UBR10K-1-INVALIDSID after reload
CSCeb26840	Cable DS CIR Problem
CSCeb27611	Ranging stops at init(i) using MC520S
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
CSCeb30765	tos-overwrite does not work on ubr10k
CSCin36219	PRE-HA: CMTS does not enforces CPE limit after the PRE switch over
CSCin37073	Untagged DS traffic does not increment native vlan counters and US t
CSCin38606	Pkts dropped after traffic policing do not incerement output drop count

Closed and Resolved Caveats for Release 12.2(11)BC3b

The caveat listed in Table 42 is resolved in Cisco IOS Release 12.2(11)BC3b. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 42 Closed and Resolved Caveats for Release 12.2(11)BC3b

Caveat ID Number	Description
CSCea30518	CMTS crashing in cmts_update_srv_flow_pak_stats
CSCea49613	PXF rate limiting dropping packets prematurely
CSCea50842	Range check missing in UCC-RSP handling
CSCea61327	Line card tracebacks after bootup
CSCea69849	SRC-VRFY: DHCP CPE loses connectivity when moved to different CM
CSCea90978	Cable modem US DS counters not retained after CM resets/flapped
CSCeb18744	sch_p2: Update ucode image to 102.0.0.19

Table 42 Closed and Resolved Caveats for Release 12.2(11)BC3b (continued)

Caveat ID Number	Description
CSCeb18926	Aggregate all BE flows on one queue per link
CSCeb24848	Col6 enq_prep table not updated for aggr queue after toaster reload

Open Caveats for Release 12.2(11)BC3a

All the caveats listed in Table 43 are open and reported in Cisco IOS Release 12.2(11)BC3a. This table lists only severity 1 and 2 caveats and select severity 3 caveats. All caveats still open in Cisco IOS Release 12.2(11)BC3 are also in Cisco IOS Release 12.2(11)BC3a.

Table 43 Open Caveats for Cisco IOS Release 12.2(11)BC3a

Caveat ID Number	Description
CSCea75288	Repeated PXF crash with due to ICMP unreachable

Closed and Resolved Caveats for Release 12.2(11)BC3a

The caveats listed in Table 44 are resolved in Cisco IOS Release 12.2(11)BC3a. 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)BC3a

Caveat ID Number	Description
CSCea65301	12.2(11)BC3 image load from 128 MB flash disk fails
CSCea73737	OC48 SRP Traffic can stop on PRE switchover

Open Caveats for Release 12.2(11)BC3

All the caveats listed in Table 45 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 45 Open Caveats for Cisco IOS Release 12.2(11)BC3

Caveat ID Number	Description
CSCdw46656	None-shared version of Downstream Frequency Override broken in 10K
CSCdw92201	Schooner: No entAliasMappingEntry for PRE1 NetworkManagementEthernet
CSCdx59958	Multi-cast fails for the CPE connected behind the slave interface
CSCdx78723	Both Working & Protect interfaces are UP with the same IP Address
CSCdy20357	16s: DSP return err_code=EC_INVALID_INUSEBAND (ACK39)
CSCdy28153	MC520S: Tracebacks observed after hw-module subslot reset
CSCdy89339	source-verify dhcp does not stop traffic for ip 0.0.0.0

Table 45 Open Caveats for Cisco IOS Release 12.2(11)BC3 (continued)

Caveat ID Number	Description
CSCdz15526	Optimization in shutting subinterface
CSCdz19043	cable privacy hotlist for manuf and cm cert not working
CSCdz23695	CPE database not updated with static IP address of new CPE until ARP
CSCdz28737	PRE-HA: Some CLIs configured on active PRE not reflected on secondary
CSCdz39744	IPC errors during boot up
CSCdz47978	MC520S:REG_REQ rejected-Multiple errors with Docsis1.0+ type config
CSCdz51438	Sch_p2: LC crashes after shut/no-shut us & clear cab modem all reset
CSCdz68844	uBR10k:Blank system messages in logs and on syslog server
CSCdz76022	uBR10k:sh int cable modem outputs incorrectly method.
CSCdz78743	Multicast doubled after HCCP switchover
CSCdz79038	PXF DMA FTC Bad Address Error with 12.2(11)CY
CSCdz85628	uBR10k: Unable to get the MIB value cdrqCmtsCmStatusTable
CSCdz85788	PXF DMA TBB Length Error with 12.2(11)CY
CSCea07227	PBR unable to be taken over
CSCea08812	CMTS keeps sending traffic on bundle intf. without m-cast members
CSCea12543	MC520:power-level CLI does not work for 3.2MHz below -4 dbmv
CSCea15929	MC520: Concatenated and Fragment packets not counted
CSCea31567	Inconsistencies in VRF arp table
CSCea34569	UBR10K-3-QUEUEFULL: Unable to enqueue since queue is full
CSCea40614	Unable to disable parser error while coping start-up config to run
CSCea41090	IGMP message should not be echoed to all interfaces in bundle
CSCea41491	sh cable modem vendor summary - shows wrong results
CSCea42352	Setting HUGE buffer to greater than 65535 takes all CLC offline
CSCea42428	cable-source verify dhcp blocks modem with valid lease
CSCea44189	sid association table shows 0.0.0.0
CSCea49613	PXF rate limiting dropping packets prematurely
CSCea50462	LC-HA: Working running consistently at 99% CPU may crash
CSCea56734	PXF crash in uBR10k
CSCea57487	LC-HA: IP address not synced to Standby PRE after N+1 switchover
CSCea59159	TOS over write does not work with BC3 but works with 11BC1
CSCin23669	scm <mac> classifier CLI counter notupdated for SF added dyn
CSCin26360	sch_p2:Spurious memory access at strcmp_mem for show controllers aft
CSCin26734	ubr10K/N+1:Dyn updated cfr not synced to protect after switchover
CSCin26768	ubr10K/N+1:Traffic matches wrong cfr on switchover followed by DSC
CSCin26829	Sch_p2:US channel change disrupts US traffic

Table 45 Open Caveats for Cisco IOS Release 12.2(11)BC3 (continued)

Caveat ID Number	Description
CSCin28584	Tracebacks observed at BigNumModEngine when CMTS switching high traf
CSCin28794	OC-12:Remote node informations are missing from the output
CSCin29305	PRE-HA: Traceback and MCASTECHO: Fail to obtain vcci for hwidb:
CSCin29431	UBR10k:Duplicate entries in show cable flap after sh/no shut on cabl
CSCin29723	UBR10K:clear cable flap <cmMacAddr> save-counters doesnot work
CSCin36219	PRE-HA: CMTS does not enforces CPE limit after the PRE switch over
CSCin37048	PRE-HA: Packets are not forwarding through secondary Dn SF after swit
CSCin37073	Untagged DS traffic does not increment native vlan counters and US t
CSCin37549	Traceback and Spurious memory access made at cmts_propagate_ip_confi
CSCin37568	Secondary PRE crashed while removing bundle from master CLC at PRE-A
CSCin38606	Pkts dropped after traffic policing do not incerement output drop co

Closed and Resolved Caveats for Release 12.2(11)BC3

The caveats listed in Table 46 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 46 Closed and Resolved Caveats for Release 12.2(11)BC3

Caveat ID Number	Description
CSCdy67959	Disk unreadable by ROMMON after format.
CSCdz06773	modems stuck in init(rc) in 1st cable bundle, 2nd ok
CSCdz14783	Traceback occurs during switchover
CSCdz32296	SNR unknown, spec group assigned, freq not assigned
CSCdz33772	Incorrect counters in show ip mroute count output w/ mroute-cache
CSCdz36174	Protect line card may crash during N+1 switch-over
CSCdz36601	Traceback at c10k_ttcm_turboacl_deconfigure_qos_acl for PBR acls
CSCdz38743	Multicast Packets punted when interface flaps
CSCdz40566	UBR10K/16S: Router crashed when running SNMP spectrum tests
CSCdz42057	cdxCmtsCmRegistered shows wrong count
CSCdz44917	OC12 SRP Card Crash During Bootup
CSCdz49701	MC520S: Spurious Memory access and traceback due to mcast sid
CSCdz50714	Spurious memory at c10k_ttcm_create_all_cmts_subints during OIR
CSCdz50750	PRE Crash at cmts_remove_bundle_entry during N+1 switchover
CSCdz52134	When slave interface added, no sh_midb for static mcast grou
CSCdz56400	10k/MC16S: freq unassigned problem with shared spectrum
CSCdz57949	PRE tty hangs on sh cable modem after hw_module_reset/switchover

Table 46 Closed and Resolved Caveats for Release 12.2(11)BC3 (continued)

Caveat ID Number	Description
CSCdz58321	Traceback when router boots up
CSCdz58875	POS connectivity failure, IPM overrun problem
CSCdz63557	MC520S: sh_midb list not updated to show the most current one
CSCdz68259	Line Card Crash at cmts_update_cm_cfr_cache, cmts_mac_timer_proc
CSCdz74433	Corrupt PC on LCP.
CSCdz75937	PXF crash when ACLs are configured
CSCdz83370	N+1: Cable LC may crash after switchover in dequeue()
CSCdz88990	Disable PRE support in latest images
CSCea00822	Need wildcard support in privilege exec setting for show/clear cable
CSCea02195	FIB leaf bitmaps not initialized correctly in RP CEF client
CSCea10721	CMTS: Cable monitor does not work on CY images
CSCea20552	continue cr10k_clc_snmp_get_us_cntr IPC timeout and some CLC not up
CSCea38653	MC520: sh int c x/x/x sid counter cannot display concant headers count
CSCea40027	High CPU on RP / large # of IPC udp sockets for RP-LC communication
CSCea42135	Input Queue full, causing many drops
CSCea44075	UBR10K: Spurious memory access when configuring bundling
CSCea44153	UBR10K: Master interface shuts down after configuring bundling
CSCin15420	Sch_p2:Spurious memory access and trace back at cmts_vencap
CSCin19953	CPE entry is not cleared when cable ip addr is removed
CSCin25167	report_malloc_failure,CPU Hog and Traceback seen with Multi
CSCin25824	Lease timer functionality does not work
CSCin26033	ubr10k/N+1:source-verify is not removed from protector after revert
CSCin26447	Traceback and assertion failure at c10k_deconfigure_if_qos
CSCin27393	SRP card flaps and tracebacks seen in show logging
CSCin29174	UBR10k:COMMIT_FAILED_ERROR on setany does not revoke the previous val
CSCin29714	UBR10K:INCONSISTENT_VALUE_ERROR on setting ccsFlapRowStatus to destroy
CSCin29842	UBR10K:Unable to reset/clear flap-list using MIB
CSCin32362	UBR10K: CMTS crashed at show_turbo_acl on issuing sh access compil
CSCin34171	UBR10K: Modems take a long time to come online
CSCin34414	PRE-HA: cable power off will cause traceback at process_ok_to_resched
CSCin35066	CMTS crashes at igmp_disable_idb when unconfiguring multicast pim
CSCin36091	CMTS crashed with rate-limiting config on SRP card
CSCin36119	PRE-HA: doing a send brk at primary will reload LC at secondary
CSCin36705	PRE-HA: AWACS Modems lose connectivity after switch-over

Table 46 Closed and Resolved Caveats for 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)BC2a

There are no open caveats specific to Cisco IOS Release 12.2(11)BC2a that require documentation in the release notes. All open caveats in Cisco IOS Release 12.2(11)BC2 are also in Cisco IOS Release 12.2(11)BC2a.

Closed and Resolved Caveats for Release 12.2(11)BC2a

The caveat listed in Table 47 is resolved in Cisco IOS Release 12.2(11)BC2a. This table describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 47 Closed and Resolved Caveats for Release 12.2(11)BC2a

Caveat ID Number	Description
CSCea04804	wrong ubr10k-p6-mz image failed CLC image loading

Open Caveats for Release 12.2(11)BC2

All the caveats listed in Table 48 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 48 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
CSCdw64361	Schooner:MC16S/CM fails to register at 160ksym/s
CSCdw92201	Schooner: No entAliasMappingEntry for PRE1 NetworkManagementEthernet
CSCdx00274	PA-FE input stuck with burst traffic
CSCdx03987	Schooner: Modems are online on a upstream not connected physical
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

Table 48 Open Caveats for Cisco IOS Release 12.2(11)BC2 (continued)

Caveat ID Number	Description
CSCdy04675	SRP Topology timer is improperly initialized
CSCdy09392	7200/16S: sh cable modem xxxx cnr does not show CNR
CSCdy11702	Ubr10k:show int cx/x/x sid association does not update after N+1 switch
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
CSCdy60261	ubr10000: LCP crash with crashinfo
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
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

Table 48 Open Caveats for Cisco IOS Release 12.2(11)BC2 (continued)

Caveat ID Number	Description
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
CSCin25496	ubr10K/N+1: RP crashed after LC fail-over. Show commands running
CSCin26033	ubr10k/N+1:source-verify is not removed from protector after revert
CSCin26408	ubr10k/N+1:Cpe database is not populated with cpe info
CSCin26734	ubr10K/N+1:Dyn updated cfr not synced to protect after switchover
CSCin26768	ubr10K/N+1:Traffic matches wrong cfr on switchover followed by DSC
CSCin27393	SRP card flaps and tracebacks seen in show logging
CSCin28359	Spurious memory access observed pas_eeprom_compare after OIR
CSCin28391	ubr10k/N+1:ping failed with source-verify dhcp after switch over

Closed and Resolved Caveats for Release 12.2(11)BC2

The caveats listed in Table 49 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 49 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
CSCdy12508	UBR10K:POS LC flaps on sending traffic and CMTS cannot ping CMs
CSCdy17114	Memory allocation failure in public buffer pools
CSCdy26782	uBR10k: CABLE MODEM QOS PROFILE cli does not work
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
CSCdy57048	Corrupted TCP packets generated by a 7206VXR
CSCdy58361	CMTS crash on watchdog timeout, process = CMTS MAC Protocol

Table 49 Closed and Resolved Caveats for Cisco IOS Release 12.2(11)BC2 (continued)

Caveat ID Number	Description
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
CSCdy76288	uBR10K:IPC failure and traceback when TCCplus card is reset
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
CSCdz11970	QOS profile max-burst range restore to 65535 for CLI
CSCdz12521	uBR10K CMTS Packet counters reset when modem reset (CLI and SNMP)
CSCdz14149	NPE-G1 returned to ROM by error - an Error Interrupt
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

Table 49 Closed and Resolved Caveats for Cisco IOS Release 12.2(11)BC2 (continued)

Caveat ID Number	Description
CSCdz32296	SNR unknown, spec group assigned, freq not assigned
CSCdz40566	UBR10K/16S: Router crashed when running SNMP spectrum tests
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 function
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 value
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 50 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 50 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 51 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 51 Open Caveats for Release 12.2(11)BC1a

Caveat ID Number	Description
CSCdy17114	Memory allocation failure in public buffer pools
CSCdz08240	UBR10k: %C10KEVENTMGR-1-MAJOR_FAULT: PXF DMA Toaster Fault
CSCdz11970	QOS profile max-burst range restore to 65535 for CLI

Table 51 Open Caveats for Release 12.2(11)BC1a (continued)

Caveat ID Number	Description
CSCdz15213	PXF crashes when tag-switching enabled
CSCdz16916	Static hosts behind CM w/ multiple IP on one MAC loose connectivity

Closed and Resolved Caveats for Release 12.2(11)BC1a

All the caveats listed in Table 52 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 52 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
CSCdz14740	Schooner: Back out CSCdy65174 - entPhysicalDescr is incorrect

Open Caveats for Release 12.2(11)BC1

All the caveats listed in Table 53 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 53 Open Caveats for Release 12.2(11)BC1

Caveat ID Number	Description
CSCdw01790	Cable MPLS VPN Arp entry in global table for VPN modem
CSCdw92201	Schooner: No entAliasMappingEntry for PRE1 NetworkManagementEthernet
CSCdx03987	Schooner: Modems are online on a upstream not connected physical
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
CSCdx92909	Schooner: modems stuck in init(rc) upon reload
CSCdy04675	SRP Topology timer is improperly initialized
CSCdy09508	linkUp trap is not sent for Cable interface upon card reinsert
CSCdy11702	Ubr10k:show int cx/x/x sid association does not update after N+1 switch
CSCdy20103	ubr10k crashed due to memory corruption

Table 53 Open Caveats for Release 12.2(11)BC1 (continued)

Caveat ID Number	Description
CSCdy26782	uBR10k: CABLE MODEM QOS PROFILE cli does not work
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
CSCdy58945	ubr10000: SNMP data mirrored across bundled interface counters
CSCdy60025	Bit fields for ToS overwrite of reversed compared to EC
CSCdy60261	ubr10000: LCP crash with crashinfo
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 54 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 54 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
CSCdw89096	Sch_p2: Hopped to incorrect freq when removed spec grp on RP
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
CSCdx62854	UBR10K: cleanup buginf in N+1
CSCdx73117	PRE Crash during N+1 switchover
CSCdx73192	C10KEVENTMGR-1-MAJOR_FAULT: PXF DMA TBB Length Error
CSCdx84066	show cable modem cable x upstream y sum 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

Table 54 Closed and Resolved Caveats for Release 12.2(11)BC1 (continued)

Caveat ID Number	Description
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
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
CSCdy30356	Schooner: Spurious access at cmts_glean
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
CSCdy52071	Schooner: Traceback at c10k_oc12pos_handle_event_msg
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

Table 54 Closed and Resolved Caveats for Release 12.2(11)BC1 (continued)

Caveat ID Number	Description
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
CSCin13206	Schooner: %SCHED-3-UNEXPECTEDEVENT: Process received unknown event

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 55 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 55 Closed and Resolved Caveats for Release 12.2(8)BC2a

Caveat ID Number	Description
CSCdy10672	TLB exception in cmts_cm_lookup
CSCdy32329	Schooner/16S: SW workaround to pass manufacturing test (CSCdy25841)

Open Caveats for Release 12.2(8)BC2

All the caveats listed in Table 56 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 56 Open Caveats for Release 12.2(8)BC2

Caveat ID Number	Description
CSCdu10291	Schooner: Output queue shows 0 even when there are lot of drops
CSCdw01790	Cable MPLS VPN Arp entry in global table for VPN modem
CSCdw64361	Schooner:MC16S/CM fails to register at 160ksym/s
CSCdw92201	Schooner: No entAliasMappingEntry for PRE1 NetworkManagementEthernet
CSCdx03987	Schooner: Modems are online on a upstream not connected physical
CSCdx25516	CM can spoof QoS once with no cable qos permission modem.
CSCdx42962	Schooner: SRP always reports slot4/0 even its in slot2/0

Table 56 Open Caveats for Release 12.2(8)BC2 (continued)

Caveat ID Number	Description
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
CSCdx59958	Schooner: mcast fails for the CPE connected behind the slave interfa
CSCdx62568	Schooner: cannot config cable match addr on sub-int for encr multica
CSCdx62698	cable host ? - cli functionality does not work with access-group
CSCdx73158	Modems Show Online on both Working & Protect Line Card
CSCdx73192	C10KEVENTMGR-1-MAJOR_FAULT: PXF DMA TBB Length Error
CSCdx78723	Both Working & Protect interfaces are UP with the same IP Address
CSCdx92909	Schooner: modems stuck in init(rc) upon reload
CSCdx93047	Crash when adding Cable Source-verify DHCP to sub-interface
CSCdx93143	sfids with minimum rate have worse performance than BE service flows
CSCdy04675	Schooner: SRP Topology timer is improperly initialized
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
CSCdy12647	Schooner: Timestamp on bootflash stored file gets modified
CSCdy15858	Change Modulation Profile Defaults: FEC codeword size
CSCdy17027	Schooner: modems stuck in init(i) following failover
CSCdy17492	Line CON 0 and VTYs cannot be cleared
CSCdy18348	PRE Crash at cmts_find_bundle_entry & cmts_bundle_pkt
CSCdy20357	16s: DSP return err_code=EC_INVALID_INUSEBAND
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 57 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 57 Closed and Resolved Caveats for Cisco IOS Release 12.2(8)BC2

Caveat ID Number	Description
CSCdv17163	Schooner: GigE status down and line-protocol down after RP reload
CSCdw50718	SNMP - snmp-set smonVlanIdStatsTable elem causes crash
CSCdx00185	CM may get IP address for PC
CSCdx04299	Schooner: Modem online with IP addr 0.0.0.0
CSCdx31307	KA timeout does not trigger callback to cops client
CSCdx37675	Many important events do not generate syslog or SNMP trap message
CSCdx40476	UBR10K: source verify CLI is rejected by CLC
CSCdx46444	automore broken when doing show cable modem remote-query
CSCdx48124	Schooner: cable bundle slave is removed in ftp.29Apr02 image
CSCdx53494	Schooner: Toaster crash on configuring in/out ACL on sub-int+bundling
CSCdx54178	Schooner: multicast fails on removing ip pim from slave
CSCdx54224	Schooner: config ACL on slave should not work
CSCdx56035	Schooner: multicast rate limit does not work
CSCdx57051	Schooner: Traceback observed during shut/no shut with HCCP configure
CSCdx57217	Error in remapping sid after HCCP revert
CSCdx57217	Error in remapping sid after HCCP revert
CSCdx57717	pppoe failed with Bundling Cable Interfaces
CSCdx57717	pppoe failed with Bundling Cable Interfaces
CSCdx58560	Display slave vcci info for bundled subints in sh hard pxf cpu sub
CSCdx58709	Schooner: modem do not pass dhcp after all the sub-int deleted
CSCdx63414	Protect Line Card Crash during N+1 Swith over
CSCdx67901	cdxIfUpChannelInputPowerLevel always returns zero as a value
CSCdx69628	With Bundling, CMTS proxy the arp for CPEs on same CM
CSCdx73117	PRE Crash during N+1 switchover
CSCdx74408	get perform snmp query using hidden community string cable-docsis
CSCdx77075	CMTS got hanged after issued sho run int Cx/y with OIR operation
CSCdx78866	Line Card Trace backs lead to keepalive failures
CSCdx81007	sho cable modem registered - CLI output shows wrong CPE information
CSCdx81051	UBR10K: Protect deletes its active subif when staticsync
CSCdx81221	Schooner: SNMP infinite loop snmpwalk
CSCdx81305	UBR10k: Memory leaks when send sync packets
CSCdx82328	Alternating ping fail failure after Worker LC is reset

Table 57 Closed and Resolved Caveats for Cisco IOS Release 12.2(8)BC2 (continued)

Caveat ID Number	Description
CSCdx86323	Schooner: show cable modem summary cmd includes non-existing intf
CSCdx89411	Traceback at cmts_dhcp_inq_reply, cmts_dhcp_glean
CSCdx92261	access-group out command on sub interfaces not synced to Protect
CSCdx94008	ACL on per-modem or per-host basis broken
CSCdx95480	uBR10012 can not obtain the docsIfCmtsServiceTable info correctly
CSCdy02319	%ERR-1-FPGA: FP FPGA bad access Error message on PRE
CSCdy06163	PRE Crash After N+1 Switch Over
CSCdy06170	Traceback & Alignment errors
CSCdy08691	DSP timeout & Acterna stop running when change mod. profile in CLI
CSCin08975	Schooner: ciscoEnvMon MIB does not return any values
CSCin09978	Schooner: SRP interface does not come up in a back to back connection

Open Caveats for Release 12.2(8)BC1

All the caveats listed in Table 58 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 58 Open Caveats for Cisco IOS Release 1.2.2(8)BC1

Caveat ID Number	Description
CSCdv17163	Schooner: GigE status down and line-protocol down after RP reload
CSCdx03987	Schooner: Modems are online on a upstream not connected physical
CSCdx16833	ubr10k - offline modems are kept more than 7 days
CSCdx45668	Redundancy state is REDUNDANCY_PEERSECONDARY_NONOPERATIONAL
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 59 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 59 Closed and Resolved Caveats for Cisco IOS Release 12.2(8)BC1

Caveat ID Number	Description
CSCdv36206	Schooner: CLC card reset due to IPC errors and MALLOCFAIL
CSCdw00626	Fantail may take a long time to boot in a fully loaded schooner
CSCdw46656	None-shared version of Downstream Frequency Override broken in 10K
CSCdw79462	CM did not become online in init(o) state w/bundling
CSCdw81195	Schooner: Traceback while doing cable power off with out TCC+ cards
CSCdw81479	Schooner: Traceback seen during reload
CSCdx01767	ubr10k; Losing Gig-e connectivity every 6-8 hours
CSCdx14085	Schooner: <IPC master:Control> port wrongly deleted on RP
CSCdx16713	Erroneous upstream IP packet causes buffer inconsistency
CSCdx16942	Cable Modem Max TX Represented by a * Instead of !
CSCdx21431	Schooner: ACL does not work for CPEs on bundle slave interface
CSCdx21896	Schooner: Multicast packets on the downstream are duplicated
CSCdx28087	Schooner: Fantail card did not get reloaded with RP reload
CSCdx30165	Schooner: output_nobuffers gets decremented with source verify on
CSCdx48124	Schooner: cable bundle slave is removed in ftp.29Apr02 image
CSCdx53494	Schooner: Toaster crash on configuring in/out ACL on sub-int+bundling
CSCdx54178	Schooner: multicast fails on removing ip pim from slave
CSCdx58709	Schooner: modem do not pass dhcp after all the sub-int deleted

Open Caveats for Release 12.2(4)BC1b

All the caveats listed in Table 60 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 60 Open Caveats for Release 12.2(4)BC1b

Caveat ID Number	Description
CSCdt25186	Schooner: int f0/0/0 always negotiates speed/duplex
CSCdu87551	Schooner: TCC+card goes down and comes up once in a while
CSCdv17163	Schooner: GigE status down and line-protocol down after RP reload
CSCdv36206	Schooner: CLC card reset due to IPC errors and MALLOCFAIL
CSCdw46656	None-shared version of Downstream Frequency Override broken in 10K
CSCdw69389	Crash at cmts_ds_trafshap_out, cal_queue_dequeue, cmts_ds_pak_handle
CSCdw81479	Schooner: Traceback seen during reload

Table 60 Open Caveats for Release 12.2(4)BC1b

Caveat ID Number	Description
CSCdw87519	Schooner: unable to ping CPE behind online CM from 1 hop or more away
CSCdx01767	ubr10k; Losing Gig-e connectivity every 6-8 hours
CSCdx04299	Schooner: Modem online with IP addr 0.0.0.0
CSCdx14085	Schooner: <IPC master:Control> port wrongly deleted on RP
CSCdx16942	Cable Modem Max TX Represented by a * Instead of !

Closed and Resolved Caveats for Release 12.2(4)BC1b

All the caveats listed in Table 61 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 61 Closed and Resolved Caveats for Release 12.2(4)BC1b

Caveat ID Number	Description
CSCdw59858	Timer Wheel Timer: crash occurred in tw_timer_replenish()
CSCdw72829	N+1 LC crashes after cli switchover
CSCdw77623	Client ip address and tty name not set in cmd author request to tac+
CSCdw78350	Spectrum-group configured gone after reload
CSCdw79462	CM did not become online in init(o) state w/bundling
CSCdw85711	Schooner: LC is up but RP puts the LC in down, because WRONGCARD
CSCdw86373	UBR7200: CALEA support
CSCdx09297	Modems show as belonging to non existent Qos Profile zero
CSCdx24998	ubr10K:DOCSIS Pingable But Not IP Pingable
CSCin04593	Schooner:MC28C/LC Crashes and the crash-info. is too big for bootflash
CSCin04772	Schooner:/MC28C Traceback seen at c10k_card_send_cmd

Open Caveats for Release 12.2(11)BC3ca

All the caveats listed in Table 62 are open in Cisco IOS Release 12.2(11)BC3ca. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 62 Open Caveats for Release 12.2(4)BC1a

Caveat ID Number	Description
CSCdt25186	Schooner: int f0/0/0 always negotiates speed/duplex
CSCdu87551	Schooner: TCC+card goes down and comes up once in a while
CSCdv17163	Schooner: GigE status down and line-protocol down after RP reload
CSCdv36206	Schooner: CLC card reset due to IPC errors and MALLOCFAIL

Closed and Resolved Caveats for Release 12.2(11)BC3ca

All the caveats listed in Table 63 are resolved in Cisco IOS Release 12.2(11)BC3ca. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

Table 63 Closed and Resolved Caveats for Release 12.2(11)BC3ca

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(11)BC3c

All the caveats listed in Table 64 are open in Cisco IOS Release 12.2(11)BC3c. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 64 Open Caveats for Release 12.2(11)BC3c

Caveat ID Number	Description
CSCdv89704	Fantail and PRE are not sync

Closed and Resolved Caveats for Release 12.2(11)BC3c

All the caveats listed in Table 65 are resolved in Cisco IOS Release 12.2(4)BC1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 65 Closed and Resolved Caveats for Release 12.2(4)BC1

Caveat ID Number	Description
CSCdv69668	Traceback received when line card ipc is disabled
CSCdv86324	Multicast forwarding does not work with cable bundling through PXF
CSCdv77670	LCP Crash when show cable modem issued
CSCdv78225	SNR formula is incorrect

Open Caveats for Release 12.2(4)XF1

All the caveats listed in Table 66 are open in Cisco IOS Release 12.2(4)XF1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 66 Open Caveats for Release 12.2(4)XF1

Caveat ID Number	Description
CSCdt25186	The PRE module's FastEthernet interface will always autonegotiate its link speed and duplex settings, even if you have manually set those parameters. This does not impact operations, however, because the interface will automatically negotiate the correct settings and come online.
CSCdu81936	An ARP packet received by the router that has the router's own interface address but with a different MAC address can overwrite the router's own MAC address in the ARP table, causing that interface to stop sending and receiving traffic. This attack is successful only against interfaces on the Ethernet segment that is local to the attacking host. The workaround for this vulnerability is to hard-code the interface's ARP table entry by using the **arp** *ip-address hardware-address type* [*alias*] command. This entry will remain in the ARP table until the **clear arp** command is issued.

CSCdu87551	Console messages similar to the following can appear on the PRE module console, indicating that the active TCC+ card has gone down and immediately come back up.
	
	`02:24:17: %IPCOIR-2-CARD_UP_DOWN: Card in slot 1/1 is down.`
	`02:24:17: %UBR10KTCC-1-NOTCC: No working TCCplus card available in the system`
	`02:24:18: %IPCOIR-5-CARD_DETECTED: Card type 2cable-tccplus (0x2AF) in slot 1/1`
	`02:24:18: %IPCOIR-2-CARD_UP_DOWN: Card in slot 1/1 is up.`
	
	These messages are generated when the PRE module misses a keepalive message from the TCC+ card, but there is no system impact because the TCC+ card is still active and running. There is no workaround.

CSCdv02247	The Cisco uBR10012 router does not support the **cable modem change-frequency**, **cable modem max-hosts**, and **cable modem qos** commands.
CSCdv17163	Under rare circumstances, a GigE line card link can go down after a PRE reload. Possible workarounds are to reenable the interface using the **shutdown** and **no shutdown** commands, or to not use autonegotiation on the link.
CSCdv17552	The cable interface line card can crash at bootup with the following message: `%CRYPTO-0-SELF_TEST_FAILURE: Encryption self-test failed.` The workaround is to reload the cable interface line card.
CSCdv36206	When a cable interface line card is under severe load, the card might generate the following error message and reload: "ipc_send_message_blocked timed_out (Cause: timeout)". The workaround is to reduce the number of cable modems on the line card.

Table 66 Open Caveats for Release 12.2(4)XF1 (continued)

Caveat ID Number	Description

CSCdv69668	A faulty external T1 reference signal can generate the following errors and reset the TCC+ card:
	`01:39:12: %UBR10KTCC-4-CHG_CLK_REF: Clock reference source changed`
	`01:39:43: %UBR10KTCC-2-LOS: Loss of signal with clock reference Primary T1`
	`01:39:43: %UBR10KTCC-4-CHG_CLK_REF: Clock reference source changed to Local oscillator`
	`01:39:56: %IPCOIR-2-CARD_UP_DOWN: Card in slot 2/1 is down.`
	`01:39:56: %IPCGRP-3-CMDOP: IPC command 19 (slot2/1): line card ipc is disabled - dropping non-blocking ipc command`

CSCdv77670	In rare circumstances, the router can crash when giving the **show cable modem** command. This can occur when a cable modem is deleted from an internal data structure at the same time the show command is accessing the data structure. There is no workaround.
CSCdv86324	Multicast packets are not forwarded to the correct slave interface in bundled interfaces. There is no workaround.
CSCdw07630	When the EIGRP or RIP routing protocols are configured on a WAN interface, and the shutdown and no shutdown commands are given on a working WAN interface to force a switchover, the routing tables are not updated to reflect the switchover to the protect interface. This does not occur during an unscheduled switchover of the interface. Possible workarounds are to use the **hccp switch** command to force a switchover instead of the **shutdown** command, or to reset the interface card.
CSCdw19230	When logging in using AAA authentication, users can enter the proper enable password but authentication can fail. The workaround is to reattempt the login, and the authentication usually then succeeds.
CSCdw25801	If the operator uses **hccp** commands to configure a live N+1 cable interface (with working and protect routers), the working interface might crash while trying to send a registration response to a modem. A workaround is to add the HCCP configuration commands at initial system provisioning, or if that is not possible, to use the **hccp lockout** command to remove the working interface from its group while configuring the interface.
CSCdw30013	When HCCP redundancy is configured, and 2000 or more cable modems are connected to a single working Cisco uBR-MC28 cable interface line card, false switch-overs can occur during moderate to high traffic conditions. The protect and working line cards will “flap” back and forth in these conditions. The workaround is to distribute the cable modems more evenly across the cable interface cards.

Closed and Resolved Caveats for Release 12.2(4)XF1

All the caveats listed in Table 67 are resolved in Cisco IOS Release 12.2(4)XF1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 67 Closed and Resolved Caveats for Release 12.2(4)XF1

Caveat ID Number	Description
CSCdv13224	In rare situations, the upstream on a slave interface in a bundle might stop passing traffic when the downstream traffic on the interface exceeds 70 kpps on a continuous basis for approximately 4 hours. The workaround is to reduce the downstream traffic below 60 kpps or so for a few moments to clear the upstream.
CSCdv86213	The router can crash at boot when adding an entry for the clock card in the SNMP MIB.
CSCdw13008	Dynamic routes that are learned through routing protocols such as RIP and OSPF are not correctly populated in the processor's routing tables, which causes those routes to be unusable during packet processing. Possible workarounds are to use static routes on the router, or to turn on tag-switching on any one interface.

Related Documentation

The following sections describe the documentation available for the Cisco uBR10012. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents. Use these release notes with these documents:

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **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*

  As a supplement to the caveats listed in "Caveats" in these release notes, see *Caveats for Cisco IOS Release 12.2*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2.

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2**: **Release Notes**: **Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **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 related documents are available on Cisco.com and the Documentation CD-ROM:

- *Cisco uBR10012 Series Hardware Installation Guide*
- *Cisco uBR10012 Series Software Configuration Guide*
- *Field Replaceable Units (FRUs)*
- *Cisco Broadband Cable Command Reference Guide*

The following documents describe the Cisco uBR-RFSW RF Switch:

- *Cisco uBR-RFSW RF Switch Installation and Configuration Guide*
- *Cisco uBR-FRSW RF Switch Cabling Instructions*
- *Cisco uBR-RFSW RF Switch Regulatory Compliance and Safety Information*

Note Some of the above documentation will not be available on Cisco.com until the official release of the Cisco uBR10012 router and its public software release.

On Cisco.com, beginning under the **Service & Support** heading:

Technical Documents: Broadband/Cable Solutions: **Cisco uBR10000 Series Universal Broadband Routers**

Note **The** *Broadband Command Consolidation* is available on Cisco.com through the following path: **Technical Documents: Broadband/Cable Solutions**

On the Documentation CD-ROM:

Cisco Product Documentation: Broadband/Cable Solutions: **Cisco uBR10000 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**

Tip Information about features of the Cisco *uBR10012* 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/ubr10k/index.htm.

Feature Modules

Feature modules describe new software enhancements, committed as features, supported by Cisco IOS Release 12.2(15)BC1, 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**: **New Feature Documentation**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **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**.

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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)