



# Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3BC

---

**Revised: February 28, 2011, OL-6760-49**

The release notes for Cisco IOS Release 12.3BC for the Cisco uBR10012 universal broadband routers describe the enhancements and caveats for all releases in the cable-specific, early deployment, 12.3BC release trains. Some of the most recent releases in 12.3BC include 12.3(17b)BCx-, 12.3(21a)BCx-, and 12.3(23)BCx-based 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 12.3(23)BC8, see the “[Caveats for Cisco IOS Release 12.3 BC](#)” section on [page 164](#) and *Caveats for Cisco IOS Release 12.3 T*. Use these release notes in conjunction with the cross-platform Release Notes for Cisco IOS Release 12.3T located on [Cisco.com](#) and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.3 T* located on [Cisco.com](#).

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at [http://www.cisco.com/en/US/customer/support/tsd\\_products\\_field\\_notice\\_summary.html](http://www.cisco.com/en/US/customer/support/tsd_products_field_notice_summary.html). If you do not have a Cisco.com login account, you can find field notices at [http://www.cisco.com/en/US/support/tsd\\_products\\_field\\_notice\\_summary.html](http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html).

## Contents

These release notes describe the following topics:

- [Early Deployment Releases, page 2](#)
- [System Requirements, page 11](#)
- [DOCSIS System Interoperability on the Cisco uBR10012 CMTS, page 14](#)
- [Feature Set Tables, page 18](#)
- [New and Changed Information, page 20](#)
- [MIBs, page 113](#)



---

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

© 2011 Cisco Systems, Inc. All rights reserved.

- [Important Notes, page 117](#)
- [Caveats for Cisco IOS Release 12.3 BC, page 164](#)
- [Related Documentation, page 770](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 773](#)

## Early Deployment Releases

These release notes describe the Cisco uBR10012 universal broadband router for Cisco IOS Release 12.3(21a)BC9, which is an early deployment (ED) release based on Cisco IOS Release 12.3 T. Early deployment releases contain fixes for software caveats and support for new Cisco hardware and software features.

[Table 1](#) shows recent early deployment releases for the Cisco uBR10012 universal broadband router.

<b>ED Release</b>	<b>Additional Software Features</b>	<b>Additional Hardware Features</b>	<b>Availability</b>
Cisco IOS Release 12.3(23)BC10	None	None	None
Cisco IOS Release 12.3(23)BC9	None	None	None
Cisco IOS Release 12.3(21a)BC9	None	None	None
Cisco IOS Release 12.3(23)BC8	None	None	None

ED Release	Additional Software Features	Additional Hardware Features	Availability
Cisco IOS Release 12.3(23)BC7	<ul style="list-style-type: none"> <li>• <a href="#">SAMIS CLC-RP Traffic Throttling</a></li> <li>• <a href="#">M-CMTS Enhancement</a></li> <li>• <a href="#">Three Step Dynamic Modulation</a></li> <li>• <a href="#">Enhanced Show Tech</a></li> <li>• <a href="#">Cable Modem QoS Information</a></li> <li>• <a href="#">Direct Load for Cable Modems</a></li> </ul> <p>The following commands are introduced in Cisco IOS Release 12.3(23)BC7:</p> <ul style="list-style-type: none"> <li>• show cable modem service-flow</li> <li>• cable upstream equalization-error-recovery</li> <li>• cable upstream threshold hysteresis</li> <li>• cable metering data-per-session</li> </ul> <p>The following commands are modified in Cisco IOS Release 12.3(23)BC7:</p> <ul style="list-style-type: none"> <li>• show tech support</li> <li>• cable upstream modulation</li> <li>• show cable hop history</li> <li>• show cr10k-rp</li> <li>• show pxf cpu queue</li> <li>• show cable metering verbose</li> <li>• cable metering destination</li> </ul> <p>See <a href="#">New Software Features in Cisco IOS Release 12.3(23)BC7</a> for details.</p>	None	Now
Cisco IOS Release 12.3(23)BC6	<p>The following command is modified in Cisco IOS Release 12.3(23)BC6:</p> <ul style="list-style-type: none"> <li>• show controllers modular-cable</li> </ul> <p>See <a href="#">New Software Features in Cisco IOS Release 12.3(23)BC6</a> for details.</p>	None	Now
Cisco IOS Release 12.3(23)BC5	<p>The following command is modified in Cisco IOS Release 12.3(23)BC5:</p> <ul style="list-style-type: none"> <li>• show controllers modular-cable</li> </ul> <p>See <a href="#">New Software Features in Cisco IOS Release 12.3(23)BC5</a> for details.</p>	None	Now
Cisco IOS Release 12.3(23)BC4	None	None	Now

ED Release	Additional Software Features	Additional Hardware Features	Availability
Cisco IOS Release 12.3(21a)BC8	None	None	Now
Cisco IO S Release 12.3(23)BC3	None	None	Now
Cisco IOS Release 12.3(23)BC2	<ul style="list-style-type: none"> <li>Subscriber Traffic Management (STM) Version 1.2</li> <li>Upstream Utilization Optimization</li> </ul>	None	Now
Cisco IOS Release 12.3(21a)BC7	None	None	Now
Cisco IOS Release 12.3(23)BC1	<ul style="list-style-type: none"> <li>PacketCable Subscriber ID Support</li> <li>MxN MAC Domain DS Load Balancing</li> <li>Line Card High Availability (HA) Support for WB Cable Modems</li> <li>Bypass the 24 Hour Timer for WB CM Use of Failed RF Channels</li> <li>Voice Support on WB Modems</li> <li>Dynamic Bandwidth Sharing for Wideband and Modular Cable Interfaces</li> </ul>	Cisco 1000BASE-T SFP Module	Now
Cisco IOS Release 12.3(21a)BC6	None	None	Now
Cisco IOS Release 12.3(21a)BC5	None	None	Now
Cisco IOS Release 12.3(23)BC	<ul style="list-style-type: none"> <li>DOCSIS 3.0 Downstream Solution</li> </ul>	<ul style="list-style-type: none"> <li>DOCSIS Timing &amp; Control Card (DTCC)</li> </ul>	Now
Cisco IOS Release 12.3(21a)BC4	None	None	Now
Cisco IOS Release 12.3(17b)BC9	None	None	Now
Cisco IOS Release 12.3(21a)BC3	<ul style="list-style-type: none"> <li>Control Point Discovery (CPD)</li> </ul>	None	Now
Cisco IOS Release 12.3(21a)BC2	None	None	Now

ED Release	Additional Software Features	Additional Hardware Features	Availability
Cisco IOS Release 12.3(21a)BC1	None	None	Now
Cisco IOS Release 12.3(21)BC	<ul style="list-style-type: none"> <li>• Automatic Virtual Interface Bundles</li> <li>• Cable DHCP Enhancements</li> <li>• Cable Duplicate MAC Address Reject</li> <li>• DOCSIS 3.0 Downstream Channel Bonding</li> <li>• Enhanced Rate Bandwidth Allocation (ERBA) on the Cisco uBR10012 Router</li> <li>• HCCP Switchover Enhancements</li> <li>• NSF Lite</li> <li>• PacketCable Client Accept Timeout</li> <li>• Per Downstream Static Multicast</li> <li>• RF Switch Firmware Version 3.60</li> <li>• Service Flow Admission Control</li> <li>• Stateful Switchover (SSO) for PacketCable and PacketCable MultiMedia</li> </ul>	<ul style="list-style-type: none"> <li>• Cisco Wideband SIP</li> <li>• Cisco Wideband SPA</li> </ul>	Now
Cisco IOS Release 12.3(17b)BC8	None	None	Now
Cisco IOS Release 12.3(17b)BC7	None	None	Now
Cisco IOS Release 12.3(17b)BC6	None	None	Now
Cisco IOS Release 12.3(17b)BC5	None	None	Now
Cisco IOS Release 12.3(17b)BC4	<ul style="list-style-type: none"> <li>• Downstream Load Balancing Distribution with Upstream Load Balancing</li> </ul>	None	Now
Cisco IOS Release 12.3(17b)BC3	None	None	Now
Cisco IOS Release 12.3(17a)BC2	<ul style="list-style-type: none"> <li>• Cisco Advanced-Mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS</li> <li>• DOCSIS1.0 TOS Overwrite</li> </ul>	None	Now

ED Release	Additional Software Features	Additional Hardware Features	Availability
Cisco IOS Release 12.3(17a)BC1	None	None	Now
Cisco IOS Release 12.3(17a)BC	<ul style="list-style-type: none"> <li>• Cable Monitor Enhancements</li> <li>• CNEM Compliance</li> <li>• Dynamic Channel Change (DCC) for Load Balancing</li> <li>• DOCSIS 2.0 SAMIS ECR Data Set</li> <li>• DSX Messages and Synchronized PHS Information</li> <li>• Generic Routing Encapsulation (GRE) Tunneling on the Cisco uBR10012</li> <li>• Globally Configured HCCP 4+1 and 7+1 Redundancy on the Cisco uBR10012 Router</li> <li>• High Availability Support for Encrypted IP Multicast</li> <li>• Management Information Base (MIB) Changes and Enhancements</li> <li>• Pre-equalization Control for Cable Modems</li> <li>• PXF ARP Filter</li> <li>• PXF Divert Rate Limiting</li> <li>• SAMIS Source Address Management</li> <li>• Secure Socket Layer Server for Usage-Based Billing</li> <li>• SSM Mapping</li> </ul>	None	Now
Cisco IOS Release 12.3(13a)BC6	None	None	Now
Cisco IOS Release 12.3(13a)BC5	None	None	Now
Cisco IOS Release 12.3(13a)BC4	None	None	Now
Cisco IOS Release 12.3(13a)BC3	None	None	Now
Cisco IOS Release 12.3(13a)BC2	None	None	Now

ED Release	Additional Software Features	Additional Hardware Features	Availability
Cisco IOS Release 12.3(13a)BC1	None	None	Now
Cisco IOS Release 12.3(13a)BC	<ul style="list-style-type: none"> <li>• Access Control List Support for COPS Intercept</li> <li>• Advanced-mode DOCSIS Set-Top Gateway Issue 1.1</li> <li>• Advanced Spectrum Management Support on the Cisco uBR10012 CMTS</li> <li>• Backup Path Testing for the Cisco RF Switch</li> <li>• Cable Monitor Support for Cisco MC5x20U-D and Cisco MC28U Broadband Processing Engines</li> <li>• COPS TCP Support for the Cisco Cable Modem Termination System</li> <li>• DHCP MAC Address Exclusion List for cable-source verify dhcp Command</li> <li>• DOCSIS 1.0 Concatenation Override</li> <li>• DOCSIS BPI+ Multiple Root Certificate Support</li> <li>• Dynamic SID/VRF Mapping Support</li> <li>• Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems</li> <li>• High Availability Features: <ul style="list-style-type: none"> <li>– Automatic Revert Feature for HCCP N+1 Redundancy Switchover Events</li> <li>– Global N+1 Redundancy</li> <li>– Shutdown and No Shutdown Enhancement for Cable Interfaces</li> </ul> </li> <li>• Low Latency Queuing (LLQ), see Optional Upstream Scheduler Modes</li> <li>• Multicast QoS Support on the Cisco uBR10012 CMTS</li> <li>• Online Offline Diagnostics (OOD) Support for the Cisco uBR10012 Universal Broadband Router</li> <li>• Optional Upstream Scheduler Modes</li> </ul>	<ul style="list-style-type: none"> <li>• Cisco Half-Height Gigabit Ethernet Line Card</li> </ul>	Now

ED Release	Additional Software Features	Additional Hardware Features	Availability
	<ul style="list-style-type: none"> <li>• <a href="#">PacketCable Emergency 911 Cable Interface Line Card Prioritization</a></li> <li>• <a href="#">PacketCable Emergency 911 Services Listing and History</a></li> <li>• <a href="#">PacketCable Multimedia for the Cisco CMTS</a></li> <li>• <a href="#">Service Independent Intercept (SII) Support</a></li> <li>• <a href="#">Subinterface support in ifTable Object</a></li> <li>• <a href="#">Transparent LAN Service and Layer 2 Virtual Private Networks</a></li> <li>• <a href="#">Virtual Interface Bundling on the Cisco uBR10-MC5X20S/U BPE</a></li> </ul>		
Cisco IOS Release 12.3(9a)BC9	None	None	Now
Cisco IOS Release 12.3(9a)BC8	None	None	Now
Cisco IOS Release 12.3(9a)BC7	None	None	Now
Cisco IOS Release 12.3(9a)BC6	None	None	Now
Cisco IOS Release 12.3(9a)BC5	None	None	Now
Cisco IOS Release 12.3(9a)BC4	None	None	Now
Cisco IOS Release 12.3(9a)BC3	None	None	Now
Cisco IOS Release 12.3(9a)BC2	None	None	Now

ED Release	Additional Software Features	Additional Hardware Features	Availability
Cisco IOS Release 12.3(9a)BC1	None	None	Now
Cisco IOS Release 12.3(9a)BC	<ul style="list-style-type: none"> <li>• Cable ARP Filter Enhancement</li> <li>• Cisco Broadband Troubleshooter 3.2</li> <li>• Cisco CMTS Static CPE Override</li> <li>• Cisco IOS Release 12.3(9a)BC Command-Line Interface (CLI) Enhancements</li> <li>• DOCSIS Set-Top Gateway Issue 1.0</li> <li>• Dynamic Shared Secret (DMIC) with OUI Exclusion, page 102</li> <li>• EtherChannel Support on the Cisco uBR10012 Universal Broadband Router</li> <li>• MIBs Changes and Updates in Cisco IOS Release 12.3(9a)BC</li> <li>• NetFlow Accounting Versions 5 and 8 Support</li> <li>• PacketCable 1.0 With CALEA</li> <li>• SFID Support for Multicast and Cable Interface Bundling</li> <li>• CBT 3.2 Spectrum Management Support with the Cisco uBR10-MC5X20S/U BPE</li> <li>• Subscriber Traffic Management (STM) Version 1.1</li> <li>• Transparent LAN Service (TLS) on the Cisco uBR10012 Router with IEEE 802.1Q</li> <li>• Usage Based Billing (SAMIS)</li> <li>• Virtual Interface and Frequency Stacking Support on the Cisco uBR10-MC5X20S/U BPE</li> <li>• Virtual Interface Support for HCCP N+1 Redundancy</li> </ul>	<ul style="list-style-type: none"> <li>• Cisco uBR10-MC5X20S /U Broadband Processing Engine</li> <li>• Cisco uBR10012 OC-48 DPT/POS Interface Module Support for the Cisco uBR10012 Performance Routing Engine 2 (PRE2) Modules</li> <li>• Cisco uBR10012 Performance Routing Engine 2 (PRE2) Modules</li> <li>• DOCSIS System Interoperability on the Cisco uBR10012 CMTS</li> </ul>	Now

# System Requirements

This section describes the system requirements for Cisco IOS Release upto 12.3(23)BC8 and includes the following sections:

- [Memory Recommendations, page 11](#)
- [Supported Hardware, page 11](#)
- [Determining the Software Version, page 17](#)
- [Determining the Software Version, page 17](#)
- [Upgrading to a New Software Release, page 17](#)
- [Feature Set Tables, page 18](#)

## Memory Recommendations

**Table 1** *Memory Recommendations for the Cisco uBR10012 Universal Broadband Router*

Platforms	Feature Sets	Cisco uBR10012 Route Processor	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco uBR10012	DOCSIS BPI IP Plus	PRE1	ubr10k-k8p6-mz	48 MB	512 MB	RAM
		PRE2	ubr10k2-k8p6-mz	48 MB	1.0 GB	RAM
	DOCSIS Base 3 DES	PRE1	ubr10k-k9p6-mz	48 MB	512 MB	RAM
		PRE2	ubr10k2-k9p6-mz	48 MB	1.0 GB	RAM

## Supported Hardware

This section describes the hardware supported by the Cisco uBR10012 Universal Broadband Router in Cisco IOS Release 12.3(21a)BC9.

For detailed descriptions of the new hardware features, see the [“New and Changed Information” section on page 20](#).

[Table 2](#) provides the list of hardware supported by the Cisco uBR10012 Universal Broadband Router.

**Table 2 Cisco uBR10012 Universal Broadband Router Supported Hardware**

Cable Interface Line Cards	<p>Up to eight of the following broadband processing engines and cable interface line cards can be housed in a chassis in any combination:</p> <ul style="list-style-type: none"> <li>• Cisco uBR10-MC5X20S/U/H Cable Interface Line Card</li> <li>• Cisco uBR10-LCP2-MC16C/MC16E/MC16S Cable Interface Line Card</li> <li>• Cisco uBR10-LCP2-MC28C Cable Interface Line Card</li> </ul> <p><b>Note</b> The Cisco uBR10-LCP2-MC16C/MC16E/MC16S and the Cisco uBR10-LCP2-MC28C are end of sale as of June 2005. For additional information, refer to END-OF-LIFE NOTICE, NO. 2600:</p> <p style="text-align: center;"><a href="http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_end-of-life_notice0900aecd80183921.html">http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_end-of-life_notice0900aecd80183921.html</a></p> <p><b>Note</b> The Cisco uBR7200 Series MC28U BPE does not support the Cisco uBR10012 router, though the Cisco MC28U BPE physically fits into the Cisco uBR10012 router chassis.</p>
Cisco Half-Height Gigabit Ethernet Line Card	<p>The Gigabit Ethernet (GigE) line card is a half-height, single-port, full-bandwidth Gigabit Ethernet line card providing multiple GigE links to the IP backbone. The Cisco half-height GigE line card also supports DOCSIS wideband capability through the Cisco uBR10000 universal broadband router.</p>
Network Uplink Line Cards	<p>Up to four line cards with any combination of the following WAN choices:</p> <ul style="list-style-type: none"> <li>• Cisco uBR10-SRP-OC12SML DPT WAN Line Card for the Cisco uBR10012 Router</li> <li>• Cisco uBR10012 OC-48 DPT/POS interface module</li> <li>• Cisco uBR10-1GE Gigabit Ethernet (GigE) uplink line card</li> <li>• Cisco uBR10-1OC12/P-SMI OC-12 POS uplink line card</li> <li>• Cisco uBR10-SRP-OC12SML Dynamic Packet Transport (DPT) WAN card</li> </ul>
Timing, Communication and Control Plus (TCC+) Card	<p>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.</p> <p>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.</p>

**Table 2 Cisco uBR10012 Universal Broadband Router Supported Hardware (continued)**

Performance Routing Engine 2 (PRE2)	<p>The new Cisco uBR10012 Series PRE2 effectively doubles the bandwidth available to each slot on the router as supported by cable interface line cards or Cisco Broadband Processing Engines.</p> <p>The PRE2 module introduces support for full-duplex Gigabit Ethernet ports, and increases the supported connections to 1.6 Gbps in full duplex (each direction per half-slot). Full-slot modules can now have up to 3.2 Gbps to and from the PRE2 module. This is twice the connection rate of the Cisco uBR10012 PRE1 route processor module.</p>
Performance Routing Engine (PRE or PRE1)	<p>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.</p> <p><b>Note</b> 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.</p> <p><b>Note</b> The Cisco uBR10012 PRE1 module supports an Ethernet port to a LAN for a 10BASE-T or 100BASE-T connection for network management. The PRE1 module supports connections of 800 Mbps in full duplex (each direction) per half-slot.</p>
AC-Input Power Entry Module (PEM)	<p>The Cisco uBR10012 router ships with two AC power entry modules (AC PEMs) that provide a redundant power supply to the system. One AC PEM can provide sufficient power for a fully configured chassis, so that if one AC PEM fails, the other automatically begins providing power for the entire router, without impacting system operations.</p> <p>The AC PEMs use standard 200–240 VAC (50/60 Hz) input power obtained through power receptacles on the front panel of each PEM. The two AC PEMs convert the AC power to provide filtered, redundant, and load shared DC power to the Cisco uBR10012 chassis.</p> <p>  <b>Caution</b> The Cisco uBR10012 router does not support mixing AC and DC PEMs. Both PEMs must be either AC PEMs or DC PEMs.</p>
DC-input Power Entry Module (PEM)	<p>The Cisco uBR10012 router may ship with two DC PEMs to 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.</p> <p>  <b>Caution</b> The Cisco uBR10012 router does not support mixing AC and DC PEMs. Both PEMs must be either AC PEMs or DC PEMs.</p>

**Table 2** Cisco uBR10012 Universal Broadband Router Supported Hardware (continued)

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 3.2 and Cisco Cable Manager 2.3.

## DOCSIS System Interoperability on the Cisco uBR10012 CMTS

This section describes the operation of primary interoperability features in the Cisco uBR10012 router. For additional DOCSIS information, refer to the following document on Cisco.com:

- DOCSIS 1.1 for the Cisco CMTS  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_docs.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html)

### Cisco IOS Release 12.3(13a)BC and DOCSIS 1.1 System Interoperability

Cisco IOS Release 12.3(13a)BC and earlier releases in this release train support several powerful new features for the Cisco uBR10012 CMTS. In addition to maintaining DOCSIS support from earlier Cisco IOS releases, Cisco IOS Release 12.3(13a)BC enhances DOCSIS support in these general categories:

- Admission Control and other features for enhanced DOCSIS Quality of Service, as provisioned by CableLabs® DOCSIS 1.1 and DOCSIS 2.0 Interface Specifications:  
<http://www.cablemodem.com/specifications/specifications20.html>
- Advanced-mode DOCSIS Set-top Gateway (A-DSG) 1.1, as provisioned by CableLabs® DOCSIS Set-top Gateway (DSG) Interface Specification, through SP-a-I03-041124, in a status of “Issued(03):  
<http://www.cablelabs.com/cablemodem/specifications/gateway.html>
- CableLabs® PacketCable 1.0 and 1.5 Support for Emergency Services and Voice  
<http://www.cablelabs.com/packetcable/specifications/>
- CableLabs® PacketCable Multimedia (PCMM):
  - PacketCable Multimedia Specification, PKT-SP-MM-I02-040930  
<http://www.cablelabs.com/packetcable/specifications/multimedia.html>

Additional High Availability and Security features as described elsewhere in this document.

## DOCSIS 1.0 Baseline Privacy

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

To enable BPI, choose software at both the CMTS and cable modem that support this mode of operation. Select a Cisco IOS image that supports BPI. BPI must be enabled using the DOCSIS configuration file.

The cable modem must also support BPI. Cable modems must have factory-installed RSA private/public key pairs to support internal algorithms to generate key pairs prior to first BPI establishment.



**Note**

---

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

---

## Cable Modem Interoperability

- The Cisco uBR10012 router supports DOCSIS 1.1-based, two-way interoperability for cable modems that support basic Internet access, Voice over IP (VoIP), or Virtual Private Networks (VPNs).
- EuroDOCSIS cable modems or set-top boxes (STBs) with integrated EuroDOCSIS CMs using Cisco uBR-MC16E cable interface line cards and Cisco IOS Release 12.2(4)BC1 or higher. EuroDOCSIS operation support includes 8-MHz Phase Alternating Line (PAL) or Systeme Electronique Couleur Avec Memoire (SECAM) channel plans.

## DOCSIS 1.0 and 1.0+ Extensions

Earlier releases of Cisco IOS software for the uBR10012 router provide support for the original DOCSIS 1.0 standard, featuring basic best-effort data traffic and Internet access over the coaxial cable network. The DOCSIS 1.0+ extensions provides Quality of Service (QoS) enhancements for real-time traffic, such as voice calls, in anticipation of full DOCSIS 1.1 support.



**Note**

---

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

---

## DOCSIS 1.1 Extensions

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

- Enhanced Quality of Service (QoS) gives priority for real-time traffic such as voice and video.
  - The DOCSIS 1.0 QoS model (a Service IDs (SID) associated with a QoS profile) has been replaced with a service flow model (SFID). This allows greater flexibility in assigning QoS parameters to different types of traffic and in responding to changing bandwidth conditions.
  - Multiple service flows per cable modem supported in either direction due to packet classifiers.

- Support for multiple service flows per cable modem allows a single cable modem to support a combination of data, voice, and video traffic.
- Greater granularity is available in QoS per cable modem (in either direction), using unidirectional service flows.
- Dynamic MAC messages are supported to create, modify, and tear down QoS service flows dynamically when requested by a DOCSIS 1.1 cable modem.
- Several QoS models are supported for the upstream.
  - Best effort-Data traffic is sent on a non-guaranteed best-effort basis.
  - Committed Information Rate (CIR) supports the guaranteed minimum bandwidth for data traffic.
  - Unsolicited Grants (UGS) support constant bit rate (CBR) traffic, such as voice, that is characterized by fixed size packets at fixed intervals.
  - Real Time Polling (rtPS) supports Real Time service flows, such as video, that produce unicast, variable size packets at fixed intervals.
  - Unsolicited Grants with Activity Detection (USG-AD) support the combination of UGS and RTPS, to accommodate real time traffic that might have periods of inactivity (such as voice using silence suppression). The service flow uses UGS fixed grants while active, but switches to RTPS polling during periods of inactivity to avoid wasting unused bandwidth.
- Enhanced time-slot scheduling mechanisms support guaranteed delay/jitter sensitive traffic on the shared multiple access upstream link.
- Payload header suppression (PHS) conserves link-layer bandwidth by suppressing unnecessary packet headers on both upstream and downstream traffic flows.
- Layer 2 fragmentation on the upstream prevents large data packets from affecting real-time traffic, such as voice and video. Large data packets are fragmented and then transmitted in the time slots that are available between the time slots used for the real-time traffic.
- Concatenation allows a cable modem to send multiple MAC frames in the same time slot, as opposed to making an individual grant request for each frame. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.
- DOCSIS 1.1 cable modems can coexist with DOCSIS 1.0 and 1.0+ cable modems in the same network—the Cisco uBR10012 router provides the levels of service that are appropriate for each cable modem.

## DOCSIS 1.1 Quality of Service

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

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

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

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

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

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

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

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco uBR10012 universal broadband router, log in to the Cisco uBR10012 universal broadband router and enter the **show version EXEC** command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) Software (uBR10k-k8p6-mz), Version 12.3(17b)BC9, EARLY DEPLOYMENT RELEASE
SOFTWARE
```

## Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, please refer to *How to Choose a Cisco IOS Software Release* at:

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1834/products\\_tech\\_note09186a00800fb9d9.shtml](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1834/products_tech_note09186a00800fb9d9.shtml)

For information about upgrading to a new software release, refer to the appropriate platform-specific document:

- Cisco uBR10012 Series Universal Broadband Routers

[http://www.cisco.com/en/US/partner/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/ubr10012/12.3\\_21\\_bc/swsipspa\\_book.html](http://www.cisco.com/en/US/partner/docs/interfaces_modules/shared_port_adapters/configuration/ubr10012/12.3_21_bc/swsipspa_book.html)

- For *Cisco IOS Upgrade Ordering Instructions*, refer to the document at the following location:

[http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957\\_pp.htm](http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm)

To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS and Catalyst OS 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 by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

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/go/fn>

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at:

<http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>

## Feature Set Tables

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.



### Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

The feature set tables have been removed from the Cisco IOS Release 12.3 release notes to improve the usability of the release notes documentation. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to 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 by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have 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](mailto: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/web/siteassets/account/index.html>

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/go/fn>

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

<http://www.cisco.com/support/FeatureNav/FNFAQ.html>

### Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.3 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

- 
- Step 1** From the Cisco Feature Navigator home page, click **Feature**.
  - Step 2** To find a feature, use either “Search by full or partial feature name” or “Browse features in alphabetical order.” Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the text box on the left side of the web page.
  - Step 3** Select a feature from the left text box, and click the **Add** button to add a feature to the Selected Features text box on the right side of the web page.




---

**Note** To learn more about a feature in the list, click the **Description** button below the left box.

---

Repeat this step to add additional features. A maximum of 20 features can be chosen for a single search.

- Step 4** Click **Continue** when you are finished selecting features.
  - Step 5** From the Major Release drop-down menu, choose **12.3**.
  - Step 6** From the Release drop-down menu, choose the appropriate maintenance release.
  - Step 7** From the Platform Family drop-down menu, select the appropriate hardware platform. The “Your selections are supported by the following:” table will list all the software images (feature sets) that support the feature(s) that you selected.
- 

### Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.3, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

- 
- Step 1** From the Cisco Feature Navigator home page, click **Compare/Release**.
  - Step 2** In the “Find the features in a specific Cisco IOS release, using one of the following methods:” box, choose **12.3** from the Cisco IOS Major Release drop-down menu.
  - Step 3** Click **Continue**.
  - Step 4** From the Release drop-down menu, choose the appropriate maintenance release.
  - Step 5** From the Platform Family drop-down menu, choose the appropriate hardware platform.
  - Step 6** From the Feature Set drop-down menu, choose the appropriate feature set. The “Your selections are supported by the following:” table will list all the features that are supported by the feature set (software image) that you selected.
-

## New and Changed Information

The following sections list the new hardware and software features supported by the Cisco uBR10012 router for Cisco IOS Release 12.3(21a)BC9:

For more information about these features, refer to the documents listed in the [“Related Documentation” section on page 770](#).

### New Hardware Features in Cisco IOS Release 12.3(23)BC10

There are no new hardware features in Cisco IOS Release 12.3(23)BC10.

### New Software Features in Cisco IOS Release 12.3(23)BC10

There are no new software features in Cisco IOS Release 12.3(23)BC10.

### New Hardware Features in Cisco IOS Release 12.3(23)BC9

There are no new hardware features supported in Cisco IOS Release 12.3(23)BC9.

### New Software Features in Cisco IOS Release 12.3(23)BC9

There are no new software features supported in Cisco IOS Release 12.3(23)BC9.

### Open Source Software Licenses for Cisco Universal Broadband Routers

For information on Open Source Software License MPL 1.1, refer to the following URL:  
[http://www.cisco.com/en/US/docs/cable/cmts/license/cable\\_licensing.html](http://www.cisco.com/en/US/docs/cable/cmts/license/cable_licensing.html)

### New Hardware Features in Cisco IOS Release 12.3(21a)BC9

There is no new hardware feature supported in Cisco IOS Release 12.3(21a)BC9.

### New Software Features in Cisco IOS Release 12.3(21a)BC9

There is no new software feature supported in Cisco IOS Release 12.3(21a)BC9.

### New Hardware Features in Cisco IOS Release 12.3(23)BC8

There is no new hardware feature supported in Cisco IOS Release 12.3(23)BC8.

## New Software Features in Cisco IOS Release 12.3(23)BC8

There is no new software feature supported in Cisco IOS Release 12.3(23)BC8.

## New Hardware Features in Cisco IOS Release 12.3(23)BC7

There is no new hardware feature supported in Cisco IOS Release 12.3(23)BC7.

## New Software Features in Cisco IOS Release 12.3(23)BC7

The following software features are new in Cisco IOS Release 12.3(23)BC7.

### SAMIS CLC-RP Traffic Throttling

The SAMIS CLC-RP traffic throttling feature limits or throttles the data collection between the cable line card and the route processor. This functionality is achieved using the new **cable metering data-per-session** command. This feature also reduces the congestion in the Broadband Processing Engine (BPE) due to the SAMIS data collection from CLC to RP.

The following commands are new or modified:

- **cable metering data-per-session**
- **show cable metering verbose**
- **cable metering destination**

### M-CMTS Enhancement

The following commands are modified in Cisco IOS Release 12.3(23)BC7. The commands are upgraded to provide better display of the route processor service flow and queue information.

- **show cr10k-rp**
- **show pxf cpu queue**

### Three Step Dynamic Modulation

Cisco IOS Release 12.3(33)BC7 introduces Three Step Dynamic Modulation, which allows you to create and use a third modulation profile in the Dynamic Upstream Modulation feature, as against the existing 16-QAM and quadrature phase-shift keying (QPSK) modulation profiles. The feature now permits 64-QAM based modulation profile to increase the upstream throughput and to satisfy the demand for new spectrum management.

The 64-QAM modulation profile is a more bandwidth-efficient modulation scheme and has a higher throughput than the other two modulation profiles.

For more details on Three Step Dynamic Modulation and the Dynamic Upstream Modulation feature, refer to *Spectrum Management and Advanced Spectrum Management for the Cisco CMTS* guide at the following location: [http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_spec.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_spec.html).

The Cisco IOS Release 12.3(23)BC7 introduces or modifies the following commands:

The **cable upstream threshold hysteresis** command was introduced to allow configurable hysteresis values for spectrum management channel upgrade thresholds.

The **cable upstream modulation** command was enhanced to accept up to three profiles, instead of the existing two.

The **show cable hop history** command was enhanced to display the modulation profile number when a change occurs.

## Enhanced Show Tech

A new keyword, **cmts**, has been added to the show tech-support command to provide debugging information specific to a cable interface or a modem for the following universal broadband routers:

- Cisco uBR10012 router
- Cisco uBR7200 series
- Cisco uBR7225VXR router

For details about this command, see the Cisco IOS CMTS Cable Command Reference at the following URL:

[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_16\\_show\\_cable\\_m\\_to\\_show\\_cable\\_u.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_16_show_cable_m_to_show_cable_u.html)

## Cable Modem QoS Information

A new command, **show cable modem service-flow**, is introduced to provide information about all service flows associated with a particular modem.

For details about this command, see the Cisco IOS CMTS Cable Command Reference at the following URL:

[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_16\\_show\\_cable\\_m\\_to\\_show\\_cable\\_u.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_16_show_cable_m_to_show_cable_u.html)

## Direct Load for Cable Modems

A new command, **cable upstream equalization-error-recovery**, is introduced to enable the CMTS to send Type-Length-Value (TLV) Type 9 in the DOCSIS RNG-RSP MAC management messages. The TLV Type 9 helps CMs come online if the TLV Type 4 convolved method causes CMs to go offline.

For details about this command, see the Cisco IOS CMTS Cable Command Reference at the following URL:

[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_10\\_cable\\_u\\_to\\_cable\\_w.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_10_cable_u_to_cable_w.html)

## New Hardware Features in Cisco IOS Release 12.3(23)BC6

There are no new hardware features supported in Cisco IOS Release 12.3(23)BC6.

## New Software Features in Cisco IOS Release 12.3(23)BC6

The following command is modified in Cisco IOS Release 12.3(23)BC6:

- show controllers modular-cable

The command output was modified to capture the SPA sensor temperature readings and error packet information.

The error information contains details about the:

- Timestamp of the captured error packet.
- Interrupt state which indicates the error type.
- Packet length.
- Blaze header part of the packet.

For additional information about this or other commands, refer to the *Cisco IOS CMTS Cable Command Reference* at [http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## New Hardware Features in Cisco IOS Release 12.3(23)BC5

There are no new hardware features supported in Cisco IOS Release 12.3(23)BC5.

## New Software Features in Cisco IOS Release 12.3(23)BC5

The following command is modified in Cisco IOS Release 12.3(23)BC5:

- show controllers modular-cable

The command output was modified to capture the SPA sensor temperature readings and error packet information.

The error information contains details about the:

- Timestamp of the captured error packet.
- Interrupt state which indicates the error type.
- Packet length.
- Blaze header part of the packet.

## New Hardware Features in Cisco IOS Release 12.3(23)BC4

There are no new hardware features supported in Cisco IOS Release 12.3(23)BC4.

## New Software Features in Cisco IOS Release 12.3(23)BC4

There are no new software features supported in Cisco IOS Release 12.3(23)BC4.

## New Hardware Features in Cisco IOS Release 12.3(21a)BC8

There are no new hardware features supported in Cisco IOS Release 12.3(21a)BC8.

## New Software Features in Cisco IOS Release 12.3(21a)BC8

There are no new software features supported in Cisco IOS Release 12.3(21a)BC8.

## New Hardware Features in Cisco IOS Release 12.3(23)BC3

There are no new hardware features supported in Cisco IOS Release 12.3(23)BC3.

## New Software Features in Cisco IOS Release 12.3(23)BC3

There are no new software features supported in Cisco IOS Release 12.3(23)BC3.

## New Hardware Features in Cisco IOS Release 12.3(23)BC2

There are no new hardware features supported in Cisco IOS Release 12.3(23)BC2.

## New Software Features in Cisco IOS Release 12.3(23)BC2

The following software features are new in Cisco IOS Release 12.3(23)BC2.

### Subscriber Traffic Management (STM) Version 1.2

The STM feature enables service providers to identify and control subscribers who exceed the maximum bandwidth allowed under their registered quality of service (QoS) profiles. STM is a simple bandwidth management tool which works as a low CPU alternative to Network-Based Application Recognition (NBAR) and access control lists (ACLs), however, using STM does not mean that NBAR and ACLs have to be turned off; STM can be applied along with NBAR and ACLs. STM also works in conjunction with the Cisco Broadband Troubleshooter to support additional network management and troubleshooting functions in the Cisco CMTS.

The STM Version 1.2 feature is enhanced in Cisco IOS Release 12.3(23)BC2 with the following support on the Cisco uBR7246VXR and Cisco uBR10012 Universal Broadband Routers:

- Support was added for the Cisco Wideband SPA (Cisco uBR10012 router only).
- Support for suspension of the cable modem (CM) penalty period at a certain time of day.
- Support for weekday and weekend traffic monitoring.
- Support of up to 40 total enforce rules.
- Support for service providers to change subscriber service classes for a particular modem using the **cable modem service-class-name** command.

Addition of the following SNMP objects to the CISCO-CABLE-QOS-MONITOR-MIB:

- ccqmCmtsEnfRulePenaltyEndTime
- ccqmCmtsEnfRuleWkndOff
- ccqmCmtsEnfRuleWkndMonDuration
- ccqmCmtsEnfRuleWkndAvgRate

- ccqmCmtsEnfRuleWkndSampleRate
- ccqmCmtsEnfRuleWkndFirstPeakTime
- ccqmCmtsEnfRuleWkndFirstDuration
- ccqmCmtsEnfRuleWkndFirstAvgRate
- ccqmCmtsEnfRuleWkndSecondPeakTime
- ccqmCmtsEnfRuleWkndSecondDuration
- ccqmCmtsEnfRuleWkndSecondAvgRate
- ccqmCmtsEnfRuleWkndOffPeakDuration
- ccqmCmtsEnfRuleWkndOffPeakAvgRate
- ccqmCmtsEnfRuleWkndAutoEnforce

The following commands are new or modified:

- cable modem service-class-name
- penalty-period
- show cable qos enforce-rule verbose
- weekend duration
- weekend off
- weekend peak-time1

For detailed information about this feature, see the *Subscriber Traffic Management on the Cisco CMTS Routers* document at:

[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_sbsbr\\_tfmgt.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_sbsbr_tfmgt.html)

## Upstream Utilization Optimization

The Upstream (US) Utilization Optimization feature on the Cisco Cable Modem Termination System (CMTS) routers provides higher upstream throughput. It provides the following benefits and functions on a Cisco CMTS router:

- Group configuration mode enables rate-adapt eligibility on all cable modem upstream flows.
- Local configuration mode enables rate-adapt eligibility on a specific upstream, provides configuration of selective parameters, and provides that local configuration overrides any global configuration.

The following commands are new or modified:

- cable upstream rate-adapt (global)
- cable upstream rate-adapt (interface)
- show cable rate-adapt
- show interface cable sid
- show interface cable upstream

For detailed information about this feature, see the *Upstream Utilization Optimization on the Cisco CMTS Routers* document at:

[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_upstream\\_rate\\_adapt.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_upstream_rate_adapt.html)

## New Hardware Features in Cisco IOS Release 12.3(21a)BC7

There are no new hardware features supported in Cisco IOS Release 12.3(21a)BC7.

## New Software Features in Cisco IOS Release 12.3(21a)BC7

There are no new software features supported in Cisco IOS Release 12.3(21a)BC7.

## New Hardware Features in Cisco IOS Release 12.3(23)BC1

The Cisco 1000BASE-T SFP module is introduced in Cisco IOS Release 12.3(23)BC1.

### Cisco 1000BASE-T SFP Module

The Cisco 1000BASE-T SFP (Small Form-Factor Pluggable) module support for the Half-Height Gigabit Ethernet Line Card is introduced in Cisco IOS Release 12.3(23)BC1. SFP modules are input/output devices that plug into a Gigabit Ethernet (GE) port to interface with a fiber-optic or copper Ethernet media. The modules are used on Cisco platforms that have Gigabit Ethernet interfaces. The product ID of the Cisco 1000BASE-T SFP module is GLC-T.

The Cisco 1000BASE-T SFP connects a Cisco Gigabit Interface Converter (GBIC) port to Category 5, Category 5e and Category 6 wiring via a standard RJ-45 interface. The maximum Category 5 wiring distance is 100m. The module provides with an option of connecting to a backhaul network interface.

The SFP-GE-T is a Copper SFP supported on the Cisco Wideband SPA. The SFP-GE-T provides full-duplex Gigabit Ethernet connectivity to high-end workstations and between wiring closets over an existing copper network infrastructure. The SFP-GE-T maximum cabling distance is 328 feet (100 m).

For more information on the Cisco 1000BASE-T SFP, see

[http://www.cisco.com/en/US/docs/routers/7200/install\\_and\\_upgrade/gbic\\_sfp\\_modules\\_install/5067g.html](http://www.cisco.com/en/US/docs/routers/7200/install_and_upgrade/gbic_sfp_modules_install/5067g.html)

For more information on the Cisco 1000 BASE-T SFP-GE-T, see

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/install\\_upgrade/uBR10012/ubrsov.html#wp1241789](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/uBR10012/ubrsov.html#wp1241789)

## New Software Features in Cisco IOS Release 12.3(23)BC1

The following software features are new in Cisco IOS Release 12.3(23)BC1.

### PacketCable Subscriber ID Support

Subscriber ID is added to all Gate Control messages and enhances error codes returned from the Cable Modem Termination System (CMTS).

Previously, the Gate ID was unique only to individual CMTS systems, with the CMTS proxying all CMS (Call Management Server) Gate control messaging through a central device which manages the CMTS connections on the behalf of the CMS. The CMS had a single Common Open Policy Service (COPS) association to the proxy device. Therefore, the Gate IDs could be duplicated when using multiple CMTS systems.

The new PacketCable Subscriber ID feature adds a Subscriber ID to each Gate Control message to disambiguate the Gate IDs between the CMS and proxy device. The Subscriber ID parameter is added to the following COPS messages:

- GATE-INFO
- GATE-DELETE
- GATE-OPEN
- GATE-CLOSE

The Subscriber ID is available at the CMS and is used in the Gate-Set messages. Additionally, the error codes returned from CMTS or its proxy are enhanced to include more specific information about gate operation failures.

To enable this feature, a new command is introduced: **packetcable gate send-subscriberID** used in global configuration mode. For more information, see the [Cisco IOS CMTS Cable Command Reference Guide](#).

## MxN MAC Domain DS Load Balancing

Prior to the introduction of this new feature, load balancing configuration using the **cable load-balance group policy** (*us-groups-across-ds*) command only considered upstream (US) load balancing across different downstream (DS) channels. This was sufficient if an US channel was not associated to more than one DS channel. However, for an MxN MAC domain, it is possible to have one US channel associated to multiple DS channels. In this case, it is necessary to further balance the DS load, once the US load is sufficiently balanced.

With the new feature, once the *us-groups-across-ds* policy is configured, CMTS attempts to balance the DS load on top of the balanced US load and among DS channels associated to the same US. The method and policy used for DS load balancing are based on the configuration in the DS load balancing group associated to the corresponding DS channels.

There are no new or modified commands for this feature.

## Line Card High Availability (HA) Support for WB Cable Modems

Wideband cable modems remain online whenever there is a failure or switchover of a 520 MD host line card, 520 guardian line card, 520 host or 520 guardian on the same line card, or a performance routing engine (PRE).

There are no new or modified commands for this feature.

## Bypass the 24 Hour Timer for WB CM Use of Failed RF Channels

When the CM sends a request to the CMTS for bonded service, the CMTS assigns the best available bonding group that is compatible with the CM. The CM then attempts to acquire the non-primary DS RF channels that are members of that bonding group. If the CM is unable to acquire one or more of the channels, it returns an error code causing the CMTS to mark all of the assigned RF channels as unacceptable for that CM. In prior versions, the channels so marked could not be reassigned to the same CM for up to 24 hours.

The new feature has removed the 24 hour timer required to clear these channels. Once the CM successfully completes registration, the list of failed RF channels for that CM is cleared. If the RF impairment has been eliminated when the CM re-registers, that channel can be reused immediately.

There are no new or modified commands for this feature.

## Voice Support on WB Modems

CMTS supports voice services on voice-enabled wideband (WB) cable modems. Committed information rate (CIR) downstream service flows on WB interfaces are supported. You can reserve up to 90% of the wideband interface bandwidth. If multiple MAC domains (MDs) are sharing a WB interface, the available link rate is distributed evenly between all MDs that share the WB interface. If the MDs that share the WB interface are on the same line card, they share the CIR pool.

To display the reserved and available bandwidth, you can use the `show-module bay all association wideband` command. To display the reserved and available bandwidth for wideband interfaces, you can use the `show interface wideband-cable` command. For more information, see the Cisco IOS CMTS Cable Command Reference Guide.

There are no new commands introduced for this feature. However, the user must first enable packet cable or multimedia packet cable to enable the voice support feature.

## Dynamic Bandwidth Sharing for Wideband and Modular Cable Interfaces

Dynamic bandwidth sharing (DBS) is the dynamic allocation of bandwidth for wideband (WB) and modular cable (MC) interfaces sharing the same downstream channel. The bandwidth available to each WB, MC, or narrowband channel is not a fixed value—it depends on the configuration and the traffic load on the WB or MC.

DBS is achieved using a new type of modality called a link queue. Link queues represent a specific share of bandwidth on a particular channel. Link queues are only used to calculate the effective bandwidth of a channel, and such link queues are activated and deactivated according to the state of activity on a specific channel. DBS and static bandwidth allocations are configured at the WB or MC interface level. By default, bandwidth for a WB or MC channel is statically allocated. When DBS is enabled on an interface, the static bandwidth percentage is converted to a committed information rate (CIR) value for the corresponding link queue. The interface CIR value represents the guaranteed portion of the interface bandwidth and is used for admission control of the service flows with minimum reserved rate. When DBS is enabled, you can also specify the remaining ratio value of the excess bandwidth for the link queue. If DBS is enabled and no bandwidth percentage is specified, no bandwidth is reserved for the WB or MC interface and the interface is effectively in protocol down state where link queues are not created.

Dynamic bandwidth sharing does not preclude static bandwidth configuration. If a static portion of bandwidth is configured on any radio frequency (RF) channel that one or more DBS-enabled channel utilizes, that portion is subtracted from the RF link's CIR. Therefore, such a portion is always reserved and is not available to dynamic WB or MC interfaces. The DBS feature continues working across line card and performance routing engine (PRE) switchovers with no loss of functionality.

For more information on the DBS please see

[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_dyn\\_bw\\_sharing.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_dyn_bw_sharing.html)

The following commands are new in Cisco IOS Release 12.3(23)BC1.

- `cable dynamic-bw-sharing`
- `debug cr10k-rp dbs-queue`
- `show pxf cable controller`

The following commands are modified in Cisco IOS Release 12.3(23)BC1.

- `cable rf-bandwidth-percent`
- `cable rf-channel`
- `show pxf cpu queue`

For a detailed description of the commands please refer the [Cisco IOS CMTS Cable Command Reference](#).

## New Hardware Features in Cisco IOS Release 12.3(21a)BC6

There are no new hardware features supported in Cisco IOS Release 12.3(21a)BC6.

## New Software Features in Cisco IOS Release 12.3(21a)BC6

There are no new software features supported in Cisco IOS Release 12.3(21a)BC6.

## New Hardware Features in Cisco IOS Release 12.3(21a)BC5

There are no new hardware features supported in Cisco IOS Release 12.3(21a)BC5.

## New Software Features in Cisco IOS Release 12.3(21a)BC5

There are no new software features supported in Cisco IOS Release 12.3(21a)BC5.

## New Hardware Features in Cisco IOS Release 12.3(23)BC

The DOCSIS Timing & Control Card (DTCC) is introduced in Cisco IOS Release 12.3(23)BC.

### DOCSIS Timing & Control Card (DTCC)

On the Cisco uBR10012 universal broadband router, the DOCSIS Timing & Control Card (DTCC) acts as a secondary processor that performs the following functions:

- In the default DTI mode, a 10.24 MHz clock and 32-bit DOCSIS timestamp are generated by the DTI Server, propagated to DTI client using DTI protocol, and distributed by DTI client to each cable interface line card.
- Allows software to independently power off any or all cable interface line cards.
- Drives the LCD panel used to display system configuration and status information.
- Monitors the supply power usage of the chassis.
- Two RJ-45 cables with the DTI server, which, in turn, can generate the clock using its own oscillator or external timing reference inputs such as GPS or network clock.

When two DTCC cards are installed, they are configured as active (primary) and backup (redundant). If the DTCC card in the first slot is working at system power-up, it automatically becomes the active card and the DTCC card in the second slot becomes the backup card. The DTCC cards monitor each other's priority information, so that if the active card fails, the active card role is transferred to the redundant backup card without loss of data.

Each DTCC card contains two RJ-45 connectors labeled Primary and Secondary, on the front panel. See [Xref\\_Colorparanum\[FC\\_FigureCap,FCW\\_FigureCapW\]](#) on page \*. These connectors are for a primary and secondary (redundant) Stratum 3 external clock reference source that is traceable to a Stratum 1

clock source. The external reference source allows the Cisco uBR10012 router's reference clock to be synchronized to the Stratum 1 clock source, providing a free-running DOCSIS-quality clock reference and time stamp to the cable interface line cards.

If present, the primary DTI link is used. If it is lost, the secondary DTI link (if present) on the active DTCC card is used. If the active DTCC card stops functioning, control is transferred to the backup DTCC card, which then uses its primary and secondary clock reference sources. If neither card has a valid clock reference source, In DTI mode, all M-CMTS elements should have common timing source. The internal clock of DTI client cannot be used to provide DOCSIS clock and timestamp. High availability strategies (active/backup card, active/backup ports) should be used to prevent loss of common timing source.

## New Software Features in Cisco IOS Release 12.3(23)BC

The following software features are new in Cisco IOS Release 12.3(23)BC:

### DOCSIS 3.0 Downstream Solution

The DOCSIS 3.0 Downstream Solution, Release 2.0, provides the following capabilities:

#### Primary-capable downstream channels from the SPA

Primary-capable channels are SPA DS channels (also known as SPA RF channels) associated with the upstream channels from the Cisco uBR10-MC5X20 line card. A SPA downstream channel is made primary-capable via Channel Grouping Domain (CGD) configuration. A primary-capable downstream channel can carry narrowband traffic as well as wideband traffic. An RF channel is considered primary-capable when it has been associated with one or more upstream channels from a Cisco uBR10-MC5X20 cable interface and this RF channel can carry DOCSIS MAC management messages (MMM) including SYNC messages, Mini-slot Allocation Packet (MAP) messages, and Upstream Channel Descriptors (UCD). They may also carry primary MAC Domain Descriptor (MDD) messages for DOCSIS 3.0 modems. Such an RF channel downstream is referred to as a primary-capable downstream. A DOCSIS Timing Interface (DTI) server which interfaces with the EQAM device and the Cisco uBR10k DTCC is used to synchronize DOCSIS MAC-layer messages. The interface represented by a single primary-capable downstream represents the narrowband portion of the RF channel.

A SPA downstream channel, whether primary-capable or not, can always be part of a bonded channel that carries bonded data traffic.

An RF channel can be shared by the associated modular-cable interface and by the wideband interfaces. The bandwidth of each RF channel can be configured to be statically divided between the modular-cable and wideband interfaces. Each RF channel's bandwidth can be used for wideband channels or narrowband channels or for a combination of the two.

A primary downstream channel is a primary-capable channel that is being used as a narrowband channel or as part of a wideband channel. A SPA downstream channel may only be a primary-capable downstream channel for a single MAC domain. However, the same SPA downstream channel may be part of one or more bonded channels (wideband interface) that serve multiple MAC domains. A primary downstream channel of one MAC domain can serve as non-primary downstream channel of another MAC domain. The total available bandwidth of a primary downstream channel, which is 96 percent, is split between the primary-capable downstream and non-primary-capable downstream channels. The remaining 4 percent is reserved for DOCSIS MAP and SYNC bandwidth.

This capability:

- Increases legacy downstream port density

- Allows legacy and bonded modems to share the same SPA DS channels
- Supports 3-channel bonding for 3-channel modems and 8-channel bonding for Linksys modems on the SPA DS channels

### Extensible MAC domain support via Channel Grouping Domain

A Channel Grouping Domain (CGD) is a collection of primary-capable downstream channels that are associated with a common set of upstream channels. A CGD is always specified within the context of a MAC domain to which all the downstream and upstream channels belong. The downstream channel local to the MAC domain on the Cisco uBR10-MC5X20 line card is always primary-capable, but a SPA downstream channel has to be made primary-capable by explicit CGD configuration. A CGD provides the additional flexibility of associating a subset of the upstream channels within a MAC domain to any of the primary-capable downstream channels, including the local downstream channels. When an upstream channel is associated with a downstream channel, its information is included in the MAP and UCD messages sent through that downstream channel. Multiple CGD configurations may be included in the same MAC domain, allowing the flexibility of the MAC domain to include various primary-capable downstream channels associated with common or different sets of upstream channels.

This capability:

- Provides support for multiple primary-capable channels per MAC domain
- Allows flexible upstream and downstream associations within a MAC domain
- Allows association of bonded channel to MAC domains

### Primary-capable downstream channel selection

Provides primary-capable downstream channel selection to facilitate channel bonding and reliability of voice-enabled modems.

#### Primary Downstream Channel Selection for Bonding Capable Modems

In order to fully utilize downstream bonding capacity, it is desired to force downstream bonding (wideband) capable modems to register on a primary-capable channel that is part of an operational downstream bonding group.

A downstream bonding capable modem is identified upon cable modem registration. A modem is downstream bonding capable if the modem reports a multiple-tuner receive capacity and a Remote Copy Protocol (RCP) known by the CMTS in REG-REQ. A wideband media terminal adapter (MTA) will be treated also as DS bonding-capable modems, therefore subject to the same primary channel selection policy.

The primary channel selection for bonding capable modems can be enabled through the global DS channel selection configuration. By default, if such configuration is not present, downstream bonding capable modems will be allowed to operate on a primary channel even it is not included in any load balancing group.

At any time after the system is up, enabling the primary channel selection for bonding capable modems will not affect existing modems in the system. The operator has to manually reset the bonding capable modems through the clear cable modem command either globally or at the per-MAC domain level.

#### Primary Downstream Channel Selection for Narrowband Modems

The primary downstream channel selection for narrowband modems is intended to provide the operator the flexibility to segregate non-bonding capable modems to specific types of DS channels with the following two options:

Redirecting Modems that Access a CMTS with Legacy DOCSIS INIT-RNG-REQ at Initialization

## Moving Non-Bonding Capable Modems to Bonding-Disabled Primary Channels

### Downstream Channel Selection for Voice-Enabled Cable Modems

This downstream channel selection option provides the operator the ability to provide high-availability for voice services by restricting voice-enabled modems to Cisco uBR10-MC5X20 downstream channels.

#### High availability

Provides high availability support for modems on SPA DS channels. The Cisco DOCSIS 3.0 Downstream Solution, Release 2.0 provides higher system availability for voice services by providing the ability to restrict voice services only to Cisco uBR10-MC5X20 line cards. This allows the CMTS to make an attempt to move the voice modems to the hosting Cisco uBR10-MC5X20 line cards of Cisco uBR10-MC5X20 downstream channels in the same load balancing group.

#### DOCSIS 1.x/2.0 and legacy feature support on SPA DS channels

Provides support for DOCSIS 1.x/2.0 modems on SPA downstream channels. The following legacy features are supported on the SPA downstream channels:

- Load balancing
- Virtual interface bundling
- Full DOCSIS Quality of Service (QoS)
- Committed Information Rate (CIR) Admission Control
- Bonded multicast
- Non-bonded multicast
- DOCSIS Set-top Gateway (DSG)
- Subscriber Accounting and Management Interface Specification (SAMIS)
- Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN)
- Baseline Privacy Interface (BPI)/Baseline Privacy Interface Plus (BPI+)
- Payload Header Suppression (PHS)
- Packet Cable and PacketCable™ Multimedia (PCMM)
- Cable modem flaplist
- Source Verify (with Dynamic Host Configuration Protocol (DHCP) option)
- Computer Assisted Law Enforcement Act (CALEA)/Service Independent Intercept (SII)/Packet Intercept
- Cable modem remote query
- DOCSIS Packet filters
- Cable Address Resolution Protocol (ARP)

#### DOCSIS 3.0 support on SPA DS channels

The Cisco DOCSIS 3.0 Downstream Solution is an industry-standard DOCSIS 3.0 implementation of channel bonding. With channel bonding, bandwidth is increased by combining or bonding multiple RF channels to create a wideband channel. The Cisco DOCSIS 3.0 Downstream Solution extensions affect the CMTS and the cable modem as well as the provisioning and network management systems. A 3-channel cable modem that performs 3-channel bonding must be able to access three SPA RF channels of which at least one RF channel must be a primary-capable channel that is used for modem registration.

The core of the Downstream 3.0 downstream solution is the sending of DOCSIS packets for a given service flow across multiple RF channels, offering significant increases in the peak downstream data rate that can be provided to a single cable modem. The transmit framer in the Cisco Wideband SPA “stripes” the DOCSIS packets for a given flow and transmits them across the multiple RF channels of the wideband channel. When the packets are received at the wideband cable modem, the modem’s receiver framer uses a sequence number embedded in each DOCSIS packet to reassemble the packets into the original flow.

The Cisco DOCSIS 3.0 Downstream Solution defines a wideband channel as a unique combination of downstream RF channels from the same SPA. The wideband CMTS manages up to 64 wideband channels (32 wideband channels per Wideband SPA). A wideband cable modem uses a wideband channel. Many wideband cable modems can share the same wideband channel.

The Cisco Wideband SPA on the Cisco uBR10012 router provides DOCSIS 3.0 channel bonding for DOCSIS Network processing. In the Cisco DOCSIS 3.0 Downstream Solution, Release 2.0, for the wideband downstream channel, the Wideband SPA uses its Gigabit Ethernet port to send data traffic to the EQAM device. This EQAM device uses one or more QAM output channels, depending on how the wideband channel is configured, to send striped packets to the wideband cable modem. In Cisco DOCSIS 3.0 Downstream Solution Release 2.0, channel bonding is used for downstream wideband channels only. A downstream wideband channel can combine up to three RF channels for a total bandwidth of over hundreds of megabits to gigabits per second with bonded modems supporting data rates of up to 292 Mbps.

In Release 2.0, channel bonding is used for downstream wideband channels only.

With the Linksys WCM300-NA modem, a downstream wideband channel can combine up to eight RF channels for a total bandwidth of up to approximately 292 Mbps (at 6 MHz and 256 QAM).

With the Scientific Atlanta DPC2505 modem, a downstream wideband channel can combine up to three RF channels for a total bandwidth of over 100 Mbps (at 6 MHz and 256 QAM).

## **New Hardware Features in Cisco IOS Release 12.3(21a)BC4**

There are no new hardware features supported in Cisco IOS Release 12.3(21a)BC4.

## **New Software Features in Cisco IOS Release 12.3(21a)BC4**

There are no new software features supported in Cisco IOS Release 12.3(21a)BC4.

## **New Hardware Features in Cisco IOS Release 12.3(17b)BC9**

There are no new hardware features supported in Cisco IOS Release 12.3(17b)BC9.

## **New Software Features in Cisco IOS Release 12.3(17b)BC9**

There are no new software features supported in Cisco IOS Release 12.3(17b)BC9.

## **New Hardware Features in Cisco IOS Release 12.3(21a)BC3**

There are no new hardware features supported in Cisco IOS Release 12.3(21a)BC3.

## New Software Features in Cisco IOS Release 12.3(21a)BC3

The following software features are new in Cisco IOS Release 12.3(21a)BC3:

### Control Point Discovery (CPD)

The Control Point Discovery (CPD) can be used to discover the IP address of a control point between the requestor and a media endpoint. It can be used by CMS (call management server), DF (delivery function for CALEA), or PS (policy server for Packetcable multimedia) to discover the IP address of the CMTS connected to the media endpoint. The CMTS needs to interpret and respond to the CPD messages.

## New Hardware Features in Cisco IOS Release 12.3(21a)BC2

There are no new hardware features supported in Cisco IOS Release 12.3(21a)BC2.

## New Software Features in Cisco IOS Release 12.3(21a)BC2

There are no new software features supported in Cisco IOS Release 12.3(21a)BC2.

## New Hardware Features in Cisco IOS Release 12.3(21a)BC1

There are no new hardware features supported in Cisco IOS Release 12.3(21a)BC1.

## New Software Features in Cisco IOS Release 12.3(21a)BC1

There are no new software features supported in Cisco IOS Release 12.3(21a)BC1.

## New Hardware Features in Cisco IOS Release 12.3(21)BC

The following hardware features are new in Cisco IOS Release 12.3(21)BC:

### Cisco Wideband SIP

The Cisco Wideband SPA interface processor (SIP) is a carrier card that inserts into a Cisco uBR10012 router slot like a line card. Each Wideband SIP supports two Cisco Wideband SPAs. The Wideband SIP provides no network connectivity on its own.

The Cisco Wideband SIP occupies two full height slots on the uBR10012 router. When the uBR1012 router is used as a wideband CMTS, slots 1/0 and 2/0 are used for the Wideband SIP. Online insertion and removal (OIR) is supported for both the Wideband SIP and the individual Wideband SPAs.

The Cisco Wideband SIP requires the Cisco uBR10012 Performance Routing Engine 2 (PRE-2).

For more information on the Cisco Wideband SIP, see the [Cisco uBR10012 Universal Broadband Router SIP and SPA Hardware Installation Guide](#).

## Cisco Wideband SPA

The Cisco Wideband shared port adapter (SPA) is a single-wide, half-height SPA that implements the DOCSIS 3.0 Downstream Channel Bonding feature. The Wideband SPA is used for downstream data traffic only. It has one active and one redundant Gigabit Ethernet port. The active port sends downstream data traffic to one or more external edge QAM devices.

The Cisco uBR10012 router can support up to two Wideband SPAs. Each Wideband SPA can support up to 12 logical wideband channels (bonding groups). Depending on how it is configured, each Wideband SPA allows up to 24 RF channels. Each logical wideband channel consists of multiple RF channels. The Cisco IOS CLI includes a set of commands to configure the Wideband SPA on the Cisco uBR10012 router.

The two Gigabit Ethernet ports on the Wideband SPA use small form-factor (SFP) modules. The SFP module is an input/output (I/O) device that plugs into a Gigabit Ethernet SFP port on the Wideband SPA, linking the port with an edge QAM device through a fiber-optic network.

For more information on the Cisco Wideband SPA, see the [Cisco uBR10012 Universal Broadband Router SIP and SPA Hardware Installation Guide](#).

## New Software Features in Cisco IOS Release 12.3(21)BC

The following software features are new in Cisco IOS Release 12.3(21)BC:

### Automatic Virtual Interface Bundles

All cable bundles are now automatically converted and configured to be in a virtual bundle, and standalone cable interfaces must be manually configured to be in a virtual bundle to operate properly.

Previously, new virtual interface bundles and bundle members required reconfiguration, and there could also be standalone interfaces not part of a bundle at all.

The following guidelines describe the automatic virtual interface bundling:

- The former rules for bundle *master* are applicable to the new *virtual bundle interface*.
- The former rules for bundle *slaves* are applicable to the new virtual bundle *members*.
- All cable bundles are automatically converted and configured to be in a virtual bundle after loading the software image.
- The virtual bundle interface accumulates the counters from members; counters on member links are not cleared when they are added to the bundle. If a bundle-only counter is desired, clear the bundle counter on the members before loading the image.
- A maximum of 40 virtual interface bundles are supported, with the numeric range from 1 to 255.
- The virtual bundle interface remains configured unless specifically deleted, even if all members in the bundle are deleted.
- This feature supports subinterfaces on the virtual bundle interface.
- *Bundle-aware* configurations are supported on the virtual bundle interface.
- *Bundle-unaware* configurations are supported on each bundle member.
- If the bundle interface existed in earlier Cisco IOS releases, the earlier cable configurations re-appear after upgrade.

For more information, see the [Cable Interface Bundling and Virtual Interface Bundling for the Cisco CMTS](#) chapter in the *Cisco CMTS Feature Guide*.

## Cable DHCP Enhancements

When using an external DHCP server, the Cisco CMTS supports a number of options that can enhance operation of the cable network in certain applications.

### Dynamic Cable Helper Address Selection

The **cable helper-address** command has been expanded to further specify where to forward DHCP packets based on origin: from a cable modem, MTA, STB, or other cable devices:

**cable helper-address** *address* [ **cable-modem** | **host** | **mta** | **stb** ]

This enables load-balancing of DHCP requests from cable modems and CPE devices by specifying different DHCP servers according to the cable interface or subinterface. You can also specify separate servers for cable modems and CPE devices.

When the **mta** or **stb** option is used, you must also use the **cable dhcp-parse option-optnum** command to parse the DHCP options.

If you specify only one option, the other types of devices (cable modem, host, mta, or stb) will not be able to connect with a DHCP server. You must specify each desired option in a separate command.

You may specify more than one helper address on each cable interface by repeating the command. You can specify more than 16 helper addresses, but the Cisco IOS software uses only the first 16 valid addresses.

If you do not specify an option, the helper-address will support all cable devices, and the associated DHCP server will accept DHCP packets from all cable device classes.

### Cable Node Location Reporting

The DHCP Relay Agent can now be used to identify cloned modems or gather geographical information for E911 and other applications. Using the **cable dhcp-insert** command, users configure the CMTS to insert downstream, upstream, or hostname descriptors into DHCP packets:

**cable dhcp-insert** { **downstream-description** | **hostname** | **upstream-description** }

A DHCP server can then utilize such information to detect cloned modems or extract geographical information. Multiple types of strings can be configured as long as the maximum relay information option size is not exceeded.

Multiple types of descriptor strings can be configured as long as the maximum relay information option size is not exceeded.

### show cable modem docsis device-class

The **show cable modem docsis device-class** command is now supported.

For more information on these enhancements and related commands, see the [Cisco Broadband Cable Command Reference Guide](#) and the "DHCP, ToD, and TFTP Services for the Cisco Cable Modem Termination System" chapter in the *Cisco CMTS Feature Guide*.

## Cable Duplicate MAC Address Reject

Cisco IOS Release 12.3(21)BC introduces a DOCSIS 1.1-compliant and above security enhancement that helps to eliminate denial-of-service (DOS) attacks that are caused by cloned cable modems. A clone is presumed to be one of two physical cable modems on the same Cisco CMTS chassis with the same HFC interface MAC address. The cloned cable modem may be DOCSIS 1.0 or greater, and may be semi-compliant or non-compliant with portions of the DOCSIS specifications.

This feature is enabled by default on the Cisco CMTS, and has no associated command-line interface (CLI) configuration commands. This feature creates a new log message. By default, this message appears in the syslog, but may be moved into the cable layer2 event log using the configuration command **cable logging layer2events**.

For additional information about this feature, its causes, and the introduction of the new **cable privacy bpi-plus-enforce** command, which enforces DOCSIS 1.1 BPI+ on the cable network, refer to the following documents on Cisco.com and the Internet:

- *Cable Duplicate MAC Address Reject for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_ccmd.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_ccmd.html)
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## DOCSIS 3.0 Downstream Channel Bonding

Cisco IOS Release 12.3(21)BC introduces the DOCSIS 3.0 Downstream Channel Bonding feature, which is the key feature of the Cisco Cable Wideband Solution, Release 1.0. This feature and the Cisco Cable Wideband Solution require the following components:

- Cisco uBR10012 router
- Cisco SIP (SPA Interface Processor) for the 1-Gbps Wideband SPA
- Cisco 1-Gbps Wideband SPA (Shared Port Adapter)

The Cisco Cable Wideband Solution, Release 1.0, also requires these major components: edge QAM (EQAM) device and wideband cable modem.

In the Cisco Cable Wideband Solution, Release 1.0, the DOCSIS 3.0 Downstream Channel Bonding feature supports downstream wideband channels consisting of multiple bonded RF channels. The solution provides wideband data services over existing hybrid fiber coax (HFC) networks. With wideband data services, multiple RF channels are aggregated into a single logical wideband channel (bonding group) that delivers higher bandwidth to the wideband cable modem than was previously possible with DOCSIS 2.0 technology. This aggregation of RF channels is referred to generically as “channel bonding.”

The Cisco Cable Wideband Solution, Release 1.0, can be deployed in parallel with DOCSIS 1.X/2.0 technology. The CMTS supports DOCSIS 1.X/2.0 modems on non-wideband ports while wideband cable modems deliver higher-speed throughput on the wideband ports.

For more information on the Cisco Cable Wideband Solution, Release 1.0, and the Cisco Wideband SIP and Cisco Wideband SPA, see these documents:

- *Cisco Cable Wideband Solution Design and Implementation Guide, Release 1.0*  
[http://www.cisco.com/en/US/docs/cable/cmts/wideband/solution/guide/release\\_1.0/wb\\_solu.html](http://www.cisco.com/en/US/docs/cable/cmts/wideband/solution/guide/release_1.0/wb_solu.html)
- *Cisco uBR10012 Universal Broadband Router SIP and SPA Hardware Installation Guide*

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/install\\_upgrade/uBR10012/hwsipsa.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/uBR10012/hwsipsa.html)

- *Cisco uBR10012 Universal Broadband Router SIP and SPA Software Configuration Guide*

[http://www.cisco.com/en/US/docs/interfaces\\_modules/shared\\_port\\_adapters/configuration/ubr10012/12.3\\_23\\_bc/sipsp\\_d3.html](http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ubr10012/12.3_23_bc/sipsp_d3.html)

## Enhanced Rate Bandwidth Allocation (ERBA) on the Cisco uBR10012 Router

Cisco IOS Release 12.3(21)BC introduces the ERBA feature on the Cisco uBR10012 CMTS with Performance Routing Engine 2 (PRE2) modules.

For additional information about ERBA in Cisco IOS Release 12.3(21)BC, refer to these documents on Cisco.com:

- *DOCSIS 1.1 for the Cisco CMTS*

[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_docs.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html)

- *Cisco IOS CMTS Cable Command Reference*

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

## HCCP Switchover Enhancements

Beginning in Cisco IOS Release 12.3(21)BC, the Cisco uBR10012 universal broadband router supports the HCCP Switchover Enhancements feature, with the following new support:

- Performance improvements for traffic recovery during line card switchover under certain scalability limits. Within the required network scalability limits, the HCCP Switchover Enhancements feature provides the following switchover benefits:
  - Less than 1-second voice call recovery.
  - Less than 20-second data recovery.
- To prevent false switchovers, the keepalive failure logic is modified.
- For faster line card switchovers, the **member subslot protect** command has been modified to add the [**config slot/subslot**] option. When using the new **config** option, you can preload upstream connectors on an HCCP protected interface to emulate the most common line card connector assignments.

The HCCP Switchover Enhancements feature in Cisco IOS Release 12.3(21)BC has the following restrictions:

- The feature is supported on the Cisco uBR10012 router with the Cisco Performance Routing Engine 2 (PRE2) only.
- The feature is supported by the following line cards on the Cisco uBR10012 router: Cisco UBR10-MC5X20S, Cisco UBR10-MC5X20U, and Cisco UBR10-MC5X20H
- The line card switchover performance improvements are valid for networks scaling to less than 5000 cable modems per line card, and less than 1000 voice calls per line card.
- The working and protect line cards must have the same channel width.
- Upconverter failure detection is not included as part of the line card switchover performance improvements.

- Virtual interface bundling is required. If you are upgrading from an earlier Cisco IOS software release and virtual bundling is not configured upon startup, the Cisco IOS software will automatically generate a virtual bundling configuration. Therefore, beginning in Cisco IOS Release 12.3(21)BC, Layer 3 information cannot be configured directly at the cable interface. The maximum number of virtual bundle interfaces supported is 40, and bundle numbers can be between 1–255.
- Tracking of HCCP interfaces is removed. The **hccp track** command is obsolete.
- In prior releases, a switchover could be triggered due to a keepalive failure no matter how many cable modems were online for an upstream. This resulted in false switchovers. In Cisco IOS Release 12.3(21)BC, keepalive failure detection is now enabled only for upstreams that have 15 or greater modems online. A switchover due to keepalive failure will trigger only if there is not any traffic on all of the upstreams associated with an interface that is enabled for keepalive.

For more information refer to the Cisco CMTS Feature Guide at:

[N+1 Redundancy for the Cisco Cable Modem Termination System](#)

## NSF Lite

The NSF Lite features RPR+ scaling and switchover performance enhancements. These enhancements will improve switchover times by keeping the Standby RP link state & Docsis(modem database) in full-sync with the Primary RP thus, enabling the Standby RP to begin forwarding traffic immediately after a switchover.

NSF Lite also provides routing enhancements for the OSPF NSF to minimize traffic outage during switchover.IDB-State Sync.

For additional information about Route Processor Redundancy Plus on the Cisco uBR10012 Universal Broadband Router, refer to the following documents on Cisco.com:

[http://www.cisco.com/en/US/products/hw/cable/ps2209/products\\_feature\\_guide09186a00801a24e0.html](http://www.cisco.com/en/US/products/hw/cable/ps2209/products_feature_guide09186a00801a24e0.html)

## PacketCable Client Accept Timeout

Cisco IOS Release 12.3(21)BC introduces support for setting timeout values for COPS Telnet connections on the Cisco CMTS, and for clearing COPS telnet sessions.

Network or Cisco CMTS telnet errors can cause incomplete COPS sessions to be created. This new timeout timer enables the clearing and cleaning of allocated resources for the stale COPS Telnet sessions on the Cisco CMTS. This feature supports COPS for PacketCable on the Cisco CMTS.

If the Connection between a PacketCable CMS and the Cisco CMTS is not completely established, and the PacketCable CMS does not correctly terminate the session by sending a TCP FIN message, the connection otherwise shows a COPS server in the output of the **show cops server** command.

The timeout timer applies to each COPS Telnet connection on the Cisco CMTS, and expiration of this timeout setting triggers the termination of the Telnet session and clears supporting resources on the Cisco CMTS.

To set the timeout timer for Telnet COPS sessions on the Cisco CMTS, use the following command in global configuration mode. To remove this timeout timer, use the **no** form of this command.

```
packetcable timer client-accept seconds
```

```
no packetcable timer client-accept seconds
```

<b>Syntax Description</b>	<i>seconds</i>	The timeout value in seconds, beyond which the Telnet COPS session is terminated, and associated resources on the Cisco CMTS are cleared.  Range from 300 seconds (five minutes) to 1800 seconds (30 minutes).
---------------------------	----------------	--

To clear all COPS Telnet sessions and associated resources on the Cisco CMTS, use the following command in global configuration mode:

**clear cops connection**

For additional information, refer to the following documents on Cisco.com:

- PacketCable and PacketCable MultiMedia for the Cisco CMTS  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_pktcable\\_mm\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- COPS Engine Operation on the Cisco CMTS  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_cops\\_eng\\_op\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_cops_eng_op_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## Per Downstream Static Multicast

The IOS IGMP Static-Group feature was first introduced back in Release 11.2, while the Source Specific Multicast (SSM) extension was added in Release 12.0(6)T. This allows network administrators to configure the router to be a statically connected member of the specified group on the interface. All multicast traffic destined to that particular group will be forwarded out on that configured interface.

Beginning in Cisco IOS Release 12.3(21)B, the Cisco uBR10012 universal broadband router supports the Per Downstream Static Multicast feature. This feature provides several multicast enhancements and makes it possible to control the replication of static IP multicast streams within a cable bundle using the **cable igmp static-group** command on the physical cable downstream interface.

For additional information, refer to the following documents on Cisco.com:

*Advanced-mode DOCSIS Set-Top Gateway 1.1 for the Cisco CMTS*

[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_docsis\\_gw12\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_docsis_gw12_ps2209_TSD_Products_Configuration_Guide_Chapter.html)

## RF Switch Firmware Version 3.60

Cisco RF Switch Firmware 3.60 is available to support N+1 Redundancy on the Cisco uBR10012 router. This Firmware version must be used with Cisco IOS Release 12.3(21)BC. Cisco RF Switch Firmware Version 3.60 provides the following changes, resolutions, enhancements, and updates:

- To help handle an increase in the SNMP traffic, Version 3.60 changes the network buffering to allocate a larger pool of (number of) buffers, with a new number of 100 buffers total.
- Version 3.60 reduces the maximum packet size to 600 bytes. This combination of a larger number of buffers with smaller maximum packet size helps with handling large bursts of inbound packets that were discarded in previous versions of Cisco RF Switch Firmware.

- Version 3.60 resolves a previous bug in the SNMP agent to help further with the above items. In prior versions of Cisco RF Switch firmware, the SNMP agent blocked traffic just after packet reception, waiting to allocate a buffer in which to place the output response. If no buffer was available (as would be the case if a large burst of incoming packets occurred), the agent would timeout, and the system would generate a watchdog timeout. Now, the agent uses a private buffer for the output response, and only requests a packet buffer after completing the snmp operation. If no buffer is available, the output response is discarded, and the agent continues processing inbound packets.
- Version 3.60 adds the **noverify** option to the **copy** command, enabling you to override the file type verification, and place a file in either the flash (FL:) or bootflash (BF:) device. Version 3.60 updates the online help to reflect this new option. This new option provides the ability to place a copy of the main application into the bootflash, so that normal system operation is restarted in the case of a system crash, instead of having the "sys>" prompt as in previous versions of Firmware.
- Version 3.60 resolves a previous issue in which concurrent access to the RF switch modules via the command-line interface and SNMP would cause random errors and crashes. The firmware now allows simultaneous usage of telnet, console, and SNMP operation. This issue was observed primarily if the show version and test module commands were used at the same time that SNMP status polling operations were occurring. This previous issue also affected a number of additional commands.

For additional information about Cisco RF Switch Firmware Version 3.60, refer to the following documents on Cisco.com:

- *Release Notes for Cisco RF Firmware, Version 3.60*  
[https://www.cisco.com/en/US/products/hw/cable/ps2929/prod\\_release\\_notes\\_list.html](https://www.cisco.com/en/US/products/hw/cable/ps2929/prod_release_notes_list.html)
- *Cisco RF Switch Firmware Configuration Guide, Version 3.60*  
[https://www.cisco.com/en/US/products/hw/cable/ps2929/products\\_installation\\_and\\_configuration\\_guides\\_list.html](https://www.cisco.com/en/US/products/hw/cable/ps2929/products_installation_and_configuration_guides_list.html)
- *Cisco RF Switch Firmware Command Reference Guide, Version 3.60*  
<https://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/command/reference/rfswcr36.html>
- *N+1 Redundancy for the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html>

## SAMIS Source Address Management

Cisco IOS Release 12.3(21)BC introduces Subscriber Account Management Interface Specification (SAMIS) enhancements which will provide the ability to set the source of the usage based billing packets originated by the router using the **cable metering** command. This enables the ip address to be set as the source of the loopback interface, similar to what is done for telnet or ftp (ip ftp source-interface0).

For additional information about Subscriber Account Management Interface Specification (SAMIS), refer to the following document on Cisco.com:

[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_sbsbr\\_tfmgt\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_sbsbr_tfmgt_ps2209_TSD_Products_Configuration_Guide_Chapter.html)

## Service Flow Admission Control

Cisco IOS Release 12.3(21)BC introduces Service Flow Admission Control (SFAC) on the Cisco Cable Modem Termination System.

SFAC on the Cisco CMTS is a mechanism that gracefully manages service flow admission requests when one or more resources are not available to process and support the incoming service request. Lack of such a mechanism not only causes the new request to fail with unexpected behavior but could potentially cause the flows that are in progress to have quality related problems. SFAC monitors such resources constantly, and accepts or denies requests depending on the resource availability.

SFAC enables you to provide a reasonable guarantee about the Quality of Service (QoS) to subscribers at the time of call admission, and to enable graceful degradation of services when resource consumption approaches critical levels. SFAC reduces the impact of unpredictable traffic demands in circumstances that would otherwise produce degraded QoS for subscribers.

SFAC uses two event types for resource monitoring and management—cable modem registration and dynamic service (voice call) requests. When either of these two events occurs on the Cisco CMTS, SFAC verifies that the associated resources conform to the configured limits prior to admitting and supporting the service call request.

SFAC is not a mechanism to apply QoS to the traffic flows. Scheduling and queuing are some of the mechanisms used for implementing the QoS. The QoS is applied on per packet basis. SFAC checks are performed before the flow is admitted.

SFAC in Cisco IOS Release 12.3(21)BC monitors the following resources on the Cisco CMTS.

- *CPU utilization*—SFAC monitors CPU utilization on the Cisco CMTS, and preserves QoS for existing service flows when new traffic would otherwise compromise CPU resources on the Cisco CMTS.
- *Memory resource utilization (I/O, Processor, and combined total)*—SFAC monitors one or both memory resources and their consumption, and preserves QoS in the same way as with CPU utilization.
- *Bandwidth utilization for upstream and downstream*—SFAC monitors upstream and downstream bandwidth utilization, and associated service classes, whether for data or dynamic service traffic.

For complete configuration and operation information, refer to the following documents on Cisco.com:

- *Service Flow Admission Control for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_svflw\\_ad\\_ctl\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_svflw_ad_ctl_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- Cisco CMTS MIB Specifications Guide  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/hw/cable/ps2209/prod_technical_reference_list.html)

## Stateful Switchover (SSO) for PacketCable and PacketCable MultiMedia

Cisco IOS Release 12.3(21)BC enhances high availability support that enables the synchronization of PacketCable and PacketCable MultiMedia (PCMM) gates during switchover events on the Cisco CMTS. This enhancement is enabled by default with Cisco IOS Release 12.3(21)BC and later supporting releases on the Cisco uBR10012 router and Cisco uBR7246VXR router.

This enhancement requires no additional configuration commands for line card redundancy in the Cisco N+1 Redundancy feature, nor the RPR+ Redundancy feature on the Cisco uBR10012 router. However, this functionality uses the existing per-interface HCCP commands that are used to associate the Working and Protect interfaces in the case of N+1 Redundancy.

This feature introduces the new **debug packetcable hccp** command to troubleshoot HCCP information specific to PacketCable and PCMM gates.

For additional information, refer to the following documents on Cisco.com:

- PacketCable and PacketCable MultiMedia for the Cisco CMTS  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_pktcable\\_mm\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *N+1 Redundancy for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_nplus1\\_redun\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_nplus1_redun_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## New Hardware Features in Cisco IOS Release 12.3(17b)BC8

There are no new hardware features supported in Cisco IOS Release 12.3(17b)BC8.

## New Software Features in Cisco IOS Release 12.3(17b)BC8

There are no new software features supported in Cisco IOS Release 12.3(17b)BC8.

## New Hardware Features in Cisco IOS Release 12.3(17b)BC7

There are no new hardware features supported in Cisco IOS Release 12.3(17b)BC7.

## New Software Features in Cisco IOS Release 12.3(17b)BC7

There are no new software features supported in Cisco IOS Release 12.3(17b)BC7.

## New Hardware Features in Cisco IOS Release 12.3(17b)BC6

There are no new hardware features supported in Cisco IOS Release 12.3(17b)BC6.

## New Software Features in Cisco IOS Release 12.3(17b)BC6

There are no new software features supported in Cisco IOS Release 12.3(17b)BC6.

## New Hardware Features in Cisco IOS Release 12.3(17b)BC5

There are no new hardware features supported in Cisco IOS Release 12.3(17b)BC5.

## New Software Features in Cisco IOS Release 12.3(17b)BC5

There are no new software features supported in Cisco IOS Release 12.3(17b)BC5.

## New Hardware Features in Cisco IOS Release 12.3(17b)BC4

The following hardware feature is new in Cisco IOS Release 12.3(17b)BC4:

### Cisco uBR10-MC5X20H Interface Line Card

Similar to the Cisco uBR10-MC5X20S and U cable interface line cards, the Cisco uBR10-MC5X20H line card is a 20 by 16 inch cards designed specifically for the Cisco uBR10012 router. It transmits and receives RF signals between the subscriber and the headend over hybrid fiber-coaxial (HFC) system.

Upstream data, from the subscriber, comes through the upstream ports (US0–US19), which the line card processes, configures and sends across the backplane to the WAN/backhaul card and out to the Internet.

Downstream data, to the subscriber, comes from the Internet through the WAN/backhaul card, and across the backplane to the cable interface line card, which processes, configures, and sends the data out through the appropriate downstream port (DS0–DS4) to be combined with the rest of the downstream signals in the headend.

The Cisco uBR10-MC5X20H line card supports both DOCSIS and EuroDOCSIS cable modem networks, in addition to downstream channels in the 70 to 860 MHz range, and upstream channels in the 5 to 65 MHz range. Each downstream port includes an onboard integrated upconverter. The cable interface line card supports Annex B and Annex A radio frequency (RF) data rates, channel widths, and modulation schemes and has DOCSIS MAC management and spectrum management capabilities. DOCSIS 2.0, A-TDMA rates are also supported.

The Cisco uBR10-MC5X20H has double the line card CPU speed, memory, and flash memory as the Cisco uBR10-MC5X20U, allowing support of Voice over IP (VoIP) at much higher call loads and a higher percentage of modems running advanced DOCSIS features that typically consume line card CPU resources.

## New Software Features in Cisco IOS Release 12.3(17b)BC4

The following software features are new in Cisco IOS Release 12.3(17b)BC4:

### Downstream Load Balancing Distribution with Upstream Load Balancing

Cisco IOS Release 12.3(17b)BC4 introduces further enhancements to downstream load balancing, resulting in equalized upstream load balancing group members. This enhancement synchronizes the pending statistic between different cable interface line cards in the load balancing group.

This enhancement performs downstream load balancing that accounts for loads on upstream channels in the same upstream load balancing group, rather than on the basis of the entire downstream channel load. Prior Cisco IOS releases may not have distributed cable modems evenly over individual upstream channels, nor in a way that accounted for downstream and upstream segment loads that account for one another.

This enhancement applies when downstream load balancing occurs on a headend system with separate upstream load balancing segments; the upstream segments are spread over multiple downstreams segments. This enhancement provides an alternative downstream load balancing scheme that accounts and makes use of per-upstream loads rather than total downstream loads.

For additional information about Load Balancing on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Load Balancing and Dynamic Channel Change on the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr\\_load-bal\\_dcc.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr_load-bal_dcc.html)
- *Cisco Broadband Cable Command Reference Guide*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## New Hardware Features in Cisco IOS Release 12.3(17b)BC3

There are no new hardware features supported in Cisco IOS Release 12.3(17b)BC3.

## New Software Features in Cisco IOS Release 12.3(17b)BC3

There are no new software features supported in Cisco IOS Release 12.3(17b)BC3.

## New Hardware Features in Cisco IOS Release 12.3(17a)BC2

There are no new hardware features supported in Cisco IOS Release 12.3(17a)BC2.

## New Software Features in Cisco IOS Release 12.3(17a)BC2

The following software features are new in Cisco IOS Release 12.3(17a)BC2:

### Cisco Advanced-Mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS

Cisco IOS Release 12.3(17a)BC2 introduces certified support for advanced-mode DOCSIS Set-Top Gateway (DSG) Issue 1.2. DSG Issue 1.2 introduces support for the latest DOCSIS Set-Top specification from CableLabs™:

- *DOCSIS Set-top Gateway (DSG) Interface Specification*, CM-SP-DSG-I05-050812

Cisco Advanced-mode DSG 1.2 is certified by CableLabs™, and is a powerful tool in support of latest industry innovations. Advanced-mode DSG 1.2 offers substantial support for enhanced DOCSIS implementation in the Broadband Cable environment. The set-top box dynamically learns the overall environment from the Cisco Cable Modem Termination System (CMTS), to include MAC address, traffic management rules, and classifiers. DSG 1.2 supports the DOCS-DSG-IF-MIB as one component of this functionality:

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

- *Advanced-mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrdsg12.html>
- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*, Rel 12.3(17a)BC2  
<http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html>

### DOCSIS1.0 ToS Overwrite

Currently, ToS overwrite requires the creation of static cable QoS profiles, which are then assigned to the ToS fields. This implementation works well if only a few different service types are offered. However, scalability issues arise when large numbers of service types are presented; each requiring a static QoS profile in order to perform ToS overwrite.

The Default DOCSIS 1.0 ToS Overwrite feature eliminates the need to create multiple QoS profiles in order to perform type-of-service (ToS) overwrite by automatically bounding all DOCSIS 1.0 Cable Modem (CM) created profiles to a default ToS overwrite.

## New Hardware Features in Cisco IOS Release 12.3(17a)BC1

There are no new hardware features supported in Cisco IOS Release 12.3(17a)BC1:

## New Software Features in Cisco IOS Release 12.3(17a)BC1

There are no new software features supported in Cisco IOS Release 12.3(17a)BC1.

## New Hardware Features in Cisco IOS Release 12.3(17a)BC

There are no new hardware features supported in Cisco IOS Release 12.3(17a)BC.

## New Software Features in Cisco IOS Release 12.3(17a)BC

The following software features are new in Cisco IOS Release 12.3(17a)BC:

- [Cable Monitor Enhancements](#)
- [CNEM Compliance](#)
- [Dynamic Channel Change \(DCC\) for Load Balancing](#)
- [DOCSIS 2.0 SAMIS ECR Data Set](#)
- [DSX Messages and Synchronized PHS Information](#)
- [Generic Routing Encapsulation \(GRE\) Tunneling on the Cisco uBR10012](#)
- [Globally Configured HCCP 4+1 and 7+1 Redundancy on the Cisco uBR10012 Router](#)
- [High Availability Support for Encrypted IP Multicast](#)
- [IPv6 over L2VPN](#)
- [Management Information Base \(MIB\) Changes and Enhancements](#)
- [Pre-equalization Control for Cable Modems](#)
- [PXF ARP Filter](#)
- [PXF Divert Rate Limiting](#)
- [Secure Socket Layer Server for Usage-Based Billing](#)
- [SSM Mapping](#)

### Cable Monitor Enhancements

Cisco IOS Release 12.3(17a)BC introduces the following enhancements to the cable monitor feature:

- Access Control Lists are now supported on the Cisco uBR-MC5X20U/D and Cisco uBR-MC28U cable interface line cards
- Unconditional downstream sniffing now enables downstream packets to be monitored, either for MAC or data packets. This enhancement supports both DOCSIS and Ethernet packet encapsulation.

For additional information about this enhancements to the cable monitor feature, refer to the following documents on Cisco.com:

- *Cable Monitor and Intercept Features on the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cmon.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html)

## CNEM Compliance

The Consistent Network Element Manageability (CNEM) Compliance feature enhances the network management capability of the CMTS platform by enabling the CMTS platform to be compliant with CNEM 1.3 requirements.

CNEM 1.3 requirements are designed to enable element management systems, with a minimum amount of effort, to maximize their coverage across the Cisco product line of network elements.

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

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html>

## DOCSIS 2.0 SAMIS ECR Data Set

The Usage-Based Billing feature for the Cisco Cable Modem Termination System (CMTS) provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. The SAMIS format is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

Release 12.3(17a)BC provides enhancements to the OSSI specifications, and billing reports (billing record format), added support to the CISCO-CABLE-METERING-MIB, which contains objects that provide subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format, added support for DCC and DCC for Load balancing and Downstream LLQ.

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

- *Usage-Based Billing for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_use-bsd\\_bill\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_use-bsd_bill_ps2209_TSD_Products_Configuration_Guide_Chapter.html)

## DSX Messages and Synchronized PHS Information

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

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

For additional information about these enhancements, and related High Availability features, refer to the following documents on Cisco.com:

- *N+1 Redundancy for the Cisco Cable Modem Termination System*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html>
- *Route Processor Redundancy Plus for the Cisco uBR10012 Router*  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/products\\_feature\\_guide09186a00801a24e0.html](http://www.cisco.com/en/US/products/hw/cable/ps2209/products_feature_guide09186a00801a24e0.html)

## Dynamic Channel Change (DCC) for Load Balancing

Cisco IOS Release 12.3(17a)BC introduces Dynamic Channel Change (DCC) and DCC for Load Balancing on the Cisco CMTS.

DCC in DOCSIS 1.1 dynamically changes cable modem upstream or downstream channels without forcing a cable modem to go offline, and without re-registration after the change. DCC supports four different initializations, instead of one, as in earlier DOCSIS support.

DCC and DCC for load balancing is supported on the Cisco uBR7246VXR router and the Cisco uBR10012 router with distributed cable interface line cards, including the Cisco MC28U and the Cisco MC5X20S/U/H.

- Load Balancing techniques allow for moving cable modems with DCC by using configurable initialization techniques.
- DCC allows line card channel changes across separate downstream channels in the same cable interface line card, with the DCC initialization techniques ranging from 0 to 4.
- DCC transfers cable modem state information from the originating downstream channel to the target downstream channel, and maintains synchronization of the cable modem information between the cable interface line card and the Network Processing Engine (NPE) or Route Processor (RP).
- When the target channel is in ATDMA mode, only DOCSIS 2.0-capable modems can be successfully load balanced. (Only DOCSIS 2.0-capable modems can operate on an ATDMA-only upstream channel.) Cisco recommends identical channel configurations in a load balancing group.

Dynamic Channel Change for Load Balancing entails the following new or enhanced commands in Cisco IOS Release 12.3(17a)BC, and later releases:

### Global Configuration Commands

- **cable load-balance group** *group-num* **dcc-init-technique** <0-4>
- **cable load-balance group** *group-num* **policy** { **pcmm** | **ugs** }
- **cable load-balance group** *group-num* **threshold** { **load** | **pcmm** | **stability** | **ugs** } <1-100>
- **cable load-balance group** *group-num* **threshold load** <1-100> { **minimum** }
- **cable load-balance group** *group-num* **threshold load** <1-100> { **enforce** }

### Testing Command

- **test cable dcc** *mac-addr* { *slot/port* | *slot/subslot/port* } *target-us-channel-id* *ranging-technique*

For configuration, command reference, testing, and examples for DCC on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Load Balancing and Dynamic Channel Change (DCC) on the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting\\_batch9/cmts1bg.html](http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting_batch9/cmts1bg.html)
- *Cisco Broadband Cable Command Reference Guide*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## Generic Routing Encapsulation (GRE) Tunneling on the Cisco uBR10012

Cisco IOS Release 12.3(17a)BC introduces Generic Routing Encapsulation (GRE) Tunneling on the Cisco uBR10012.

Generic Route Encapsulation (GRE) is a tunneling protocol that can encapsulate a variety of packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

## Globally Configured HCCP 4+1 and 7+1 Redundancy on the Cisco uBR10012 Router

Cisco IOS Release 12.3(17a)BC introduces support for globally-configured HCCP N+1 Redundancy on the Cisco uBR10012 router. Cisco IOS Release 12.3(17a)BC supports both 4+1 and 7+1 Redundancy, in these High Availability configurations:

- 7+1 Redundancy, supporting the Cisco uBR10012 router with two Cisco RF Switches

In this configuration, seven Working cable interface line cards are supported by one Protect cable interface line card. Two Cisco RF Switches are connected to seven MC5X20U/D cable interface line cards. Switchover events apply to an entire line card, rather than on an interface level, as in previous Cisco IOS releases supporting 7+1 Redundancy. Global configuration makes this High Availability feature easier to configure and use. 7+1 Redundancy is the default redundancy scheme for the Cisco uBR10012 router in Cisco IOS Release 12.3(17a)BC.

- 4+1 Redundancy, supporting the Cisco uBR10012 router with one Cisco RF Switch

In this configuration, four Working cable interface line cards are supported by one Protect line card. One Cisco RF Switch is connected to five cable interface line cards. Switchover events apply to an entire line card.

Either form of N+1 Redundancy supports the Cisco uBR-MC5X20U/D broadband processing engine (BPE) on the Cisco uBR10012 router.



### Note

N+1 Redundancy requires that all BPEs in the Cisco uBR10012 router be the same. Only the Cisco uBR-MC5X20U/D BPE is supported.



### Note

Cisco IOS Release 12.3(17a)BC introduces simplified global configuration commands, supporting 4+1 or 7+1 Redundancy on the Cisco uBR10012 router. However, earlier configuration commands are not supported when Global-level N+1 Redundancy is configured on the Cisco uBR10012 router.

For additional information about HCCP 4+1 Redundancy, refer to the following document on Cisco.com:

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

## High Availability Support for Encrypted IP Multicast

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

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

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html>
- *Dynamic Shared Secret for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_dyn\\_sh\\_sec\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_dyn_sh_sec_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *IP Multicast in Cable Networks*, White Paper  
[http://www.cisco.com/en/US/technologies/tk648/tk828/technologies\\_case\\_study0900aecd802e2ce2.html](http://www.cisco.com/en/US/technologies/tk648/tk828/technologies_case_study0900aecd802e2ce2.html)
- *N+1 Redundancy for the Cisco Cable Modem Termination System*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_nplus1\\_redun\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_nplus1_redun_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *Route Processor Redundancy Plus for the Cisco uBR10012 Router*  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/products\\_feature\\_guide09186a00801a24e0.html](http://www.cisco.com/en/US/products/hw/cable/ps2209/products_feature_guide09186a00801a24e0.html)

## IPv6 over L2VPN

Beginning with Cisco IOS Release 12.3(17a)BC, the Cisco uBR10012 router now supports IPv6 using Layer 2 VPNs based on SID to 802.1q mapping. The Cisco uBR10012 router already supported Transparent LAN service with Layer 2 VPNs in Cisco IOS Release 12.3(13a)BC and later releases. As more Internet users switch to IPv6, the Cisco IPv6 protocol support helps enable the transition. IPv6 fixes a number of limitations in IPv4, such as limited numbers of available IPv4 addresses in addition to improved routing and network auto-configuration. This feature allows customers to introduce IPv6 into their network with minimal operational impact.

For additional information about this feature, refer to the following documents on Cisco.com:

- IPv6 Documentation: overview, technology, design and configuration information  
[http://www.cisco.com/en/US/tech/tk872/tsd\\_technology\\_support\\_protocol\\_home.html](http://www.cisco.com/en/US/tech/tk872/tsd_technology_support_protocol_home.html)

## Management Information Base (MIB) Changes and Enhancements

MIB enhancements in Cisco IOS Release 12.3(17a)BC provide enhanced management features that enable the Cisco uBR 7200 Series router and the Cisco uBR10012 router to be managed through the Simple Network Management Protocol (SNMP). These enhanced management features allow you to:

- Use SNMP set and get requests to access information in Cisco CMTS universal broadband routers.
- Reduce the amount of time and system resources required to perform functions like inventory management.
- A standards-based technology (SNMP) for monitoring faults and performance on the router.

- Support for SNMP versions (SNMPv1, SNMPv2c, and SNMPv3).
- Notification of faults, alarms, and conditions that can affect services.

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

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html>

## Pre-equalization Control for Cable Modems

Cisco IOS Release 12.3(17a)BC introduces pre-equalization control for cable modems on a per-modem basis. This feature enhances support for pre-equalization control on an interface basis, using the Organizational Unique Identifier (OUI), which is also supported.

When pre-equalization is enabled on an upstream interface, this feature allows you to disable pre-equalization adjustment selectively, for a specific cable modem or a group of cable modems. This feature prevents cable modems from flapping when processing pre-equalization requests sent from the Cisco CMTS.

### Restrictions

This feature observes the following restrictions in Cisco IOS Release 12.3(17a)BC:

- For pre-equalization to be supported on a per-modem basis, the cable modem must send verification of pre-equalization after it registers with the Cisco CMTS.
- The option of excluding the OUI is a global configuration. For the cable modem on which OUI is excluded, the excluded OUI is disabled for all interfaces. This method uses a list of OUI values, recording which modems are sent and not sent pre-equalization.

### able pre-equalization exclude

To exclude a cable modem from pre-equalization during registration with the Cisco CMTS, use the **cable pre-equalization exclude** command in global configuration mode. Exclusion is supported for a specified cable modem, or for a specified OUI value for the entire interface. To remove exclusion for the specified cable modem or interface, use the **no** form of this command. Removing this configuration returns the cable modem or interface to normal pre-equalization processes during cable modem registration.

```
cable pre-equalization exclude {oui | modem} mac-addr
```

```
no cable pre-equalization exclude {oui | modem} mac-addr
```

### Syntax Description

<b>oui</b>	Organizational Unique identifier for the interface specified. Using this keyword excludes the specified OUI during cable modem registration for the associated interface.
<b>modem</b>	Cable Modem identifier for the cable modem specified. Using this keyword excludes the cable modem.
mac-addr	Identifier for the OUI or cable modem to be excluded.

**Command Default**

Pre-equalization is enabled by default on the Cisco router, and for cable modems that have a valid and operational DOCSIS configuration file. When enabled, pre-equalization sends ranging messages for the respective cable modems. When disabled with the new **exclude** command, pre-equalization is excluded for the respective cable modems.

**Command Modes**

Global configuration mode

**Command History**

Release	Modification
12.3(17a)BC	This command was introduced to the Cisco uBR10012 router and the Cisco uBR7246VXR router.

**Usage Guidelines**

The pre-equalization exclusion feature should be configured for the running configuration of the Network Processing Engine (NPE), the Performance Routing Engine (PRE), and the line card console.

**Examples**

The following example configures pre-equalization to be excluded for the specified cable modem. Pre-equalization data is not sent for the corresponding cable modem:

```
Router(config)# cable pre-equalization exclude modem mac-add
```

The following example configures pre-equalization to be excluded for the specified OUI value of the entire interface. Pre-equalization data is not sent for the corresponding OUI value of the entire interface:

```
Router(config)# cable pre-equalization exclude oui mac-addr
```

The following series of commands configures pre-equalization on the Cisco uBR10012 router with MC5X20U BPEs. On the PRE Console, configure the following commands.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable pre-equalization exclude oui 00.09.04
Router(config)# end
Router# show run
Router# show running-config | inc oui
cable pre-equalization exclude oui 00.09.04
```

On the line card console for the same Cisco uBR10012 router, verify the configuration with the following command:

```
Router# show running-config | inc oui
cable pre-equalization exclude oui 00.09.04
```

The following series of commands configures pre-equalization on the Cisco uBR72436VXR router with MC28U cable interface line cards. On the Network Processing Engine (NPE) console, configure and verify with the following commands.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable pre-equalization exclude oui 00.09.24
Router(config)# end
Router# show run
02:58:10: %SYS-5-CONFIG_I: Configured from console by consolen
Router# show running-config | inc oui
cable pre-equalization exclude oui 00.09.24
```

On the line card console for the same Cisco uBR7246VXR router, verify the configuration with the following command:

```
Router# show running-config | inc oui
cable pre-equalization exclude oui 00.09.24
```

After either of these exclusion methods for pre-equalization are configured, you can verify that all ranging messages do not include pre-equalization data. Use the following debug commands in global configuration mode:

- **debug cable range**
- **debug cable interface** cx/x/x mac-addr

Verify the ranging message for the non-excluded cable modems include pre-equalization data, and for the excluded cable modems, the ranging messages do not include such data.

The following example removes pre-equalization exclusion for the specified OUI and interface. This results in the cable modem or OUI to return to normal pre-equalization functions. Ranging messages resume sending pre-equalization data.

```
Router(config)# no cable pre-equalization exclude { oui | modem } mac-addr
Removal of this feature can be verified with the following debug command:
```

- **debug cable interface** cx/x/x mac-ad—Verifies the ranging message for all non-excl modems include pre-eq data, and for the excluded modems ranging messages do not include pre-eq data.

For additional information about this or other commands, refer to the following documents on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)
- *DOCSIS 1.1 for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_docs.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html)

## PXF ARP Filter

Cisco IOS Release 12.3(17a)BC introduces PXF ARP Filter feature. The ARP filter now has a PXF component that filters ARP packets for identified “ARP offenders”, thereby decreasing ARP punt rate and RP CPU usage.

For additional information, refer to the following document on Cisco.com

- *Cable ARP Filtering*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_cbl\\_arp\\_fltr\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_cbl_arp_fltr_ps2209_TSD_Products_Configuration_Guide_Chapter.html)

## PXF Divert Rate Limiting

Cisco IOS Release 12.3(17a)BC introduces PXF Divert Rate Limiting feature. Rate-limiting on the divert path causes packets that will cause congestion to toRP queues to be dropped, before any packets have been queued, so valid packets are unaffected.

For additional information, refer to the following document on Cisco.com

- *Cable ARP Filtering*

[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_cbl\\_arp\\_fltr\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_cbl_arp_fltr_ps2209_TSD_Products_Configuration_Guide_Chapter.html)

## show cable modem Command Changes

Cisco IOS Release 12.3(17a)BC introduces changes for two versions of the **show cable modem** command.

- **show cable modem mac summary**

The information displayed with this command is revised. The DOCSIS 2.0 column in the Quality of Service (QoS) Provision Mode field has been removed, as this field is not applicable to QoS provisioning in DOCSIS 2.0.

### Command Output in Cisco IOS Release 12.3(17a)BC and Later Releases

```
Router# show cable modem mac summary
                        Cable Modem Summary
                        -----
                        Mac Version                QoS Provision Mode
Interface      Total  DOC2.0  DOC1.1  DOC1.0  Reg/Online  DOC1.1  DOC1.0
Cable5/1/0/U0  10     0       2       8       10         0       10
```

### Command Output in Cisco IOS Release 12.3(13a)BC and Earlier Releases

```
Router# show cable modem mac summary
                        Cable Modem Summary
                        -----
                        Mac Version                QoS Provision Mode
Interface      Total  DOC2.0  DOC1.1  DOC1.0  Reg/Online  DOC2.0  DOC1.1  DOC1.0
Cable8/0/0/U0  8     0       5       3       5         0       5       0
```

- **show cable modem phy**

The information displayed with this command is revised. The MicroReflec column (MicroReflections) has been removed, and the DOCSIS Prov (DOCSIS Provider) column has been added in its place. This new column contains DOCSIS version information.

### Command Output in Cisco IOS Release 12.3(17a)BC and Later Releases

```
Router#show cable modem phy
MAC Address      I/F      Sid  USPwr  USSNR  Timing  DSPwr  DSSNR  Mode  DOCSIS
                I/F      Sid  (dBmV) (dB)  Offset (dBmV) (dB)  Prov
0003.e350.9a3f  C5/1/0/U0  1    0.00  30.23  2811   0.00  -----  tdma  1.0
0050.734e.c1a1  C5/1/0/U0  2    0.00  30.47  2811   0.00  -----  tdma  1.0
0007.0e01.1749  C5/1/0/U0  3    0.00  30.65  2808   0.00  -----  tdma  1.0
0007.0e00.90dd  C5/1/0/U0  4    0.00  30.66  2806   0.00  -----  tdma  1.0
0003.e350.9ad3  C5/1/0/U0  5    0.00  30.47  2810   0.00  -----  tdma  1.0
0003.e38f.f4e5  C5/1/0/U0  6    0.00  30.36  2813   0.00  -----  tdma  1.0
0003.e350.9b97  C5/1/0/U0  7    0.00  30.44  2812   0.00  -----  tdma  1.0
0003.e350.9bed  C5/1/0/U0  8    0.00  30.16  2814   0.00  -----  tdma  1.0
0003.e308.455d  C5/1/0/U0  9    0.00  30.79  2811   0.00  -----  tdma  1.0
0003.6bd6.bfaf  C5/1/0/U0  10   0.00  30.40  2813   0.00  -----  tdma  1.0
```

**Command Output in Cisco IOS Release 12.3(13a)BC and Earlier Releases**Router#**show cable modem phy**

MAC Address	I/F	Sid	USPwr (dBmV)	USSNR (dB)	Timing Offset	MicroReflec (dBc)	DSPwr (dBmV)	DSSNR (dB)	Mode
0008.0e06.7b14	C8/0/0/U0	1	0.00	30.36	1938	0	0.00	-----	tdma
0050.f112.5977	C8/0/0/U0	2	0.00	30.36	1695	0	0.00	-----	tdma
0090.837b.b0b9	C8/0/0/U0	3	0.00	30.64	1187	0	0.00	-----	tdma
0007.0e03.6e99	C8/0/0/U0	5	0.00	30.36	2747	0	0.00	-----	tdma
0007.0e04.5091	C8/0/0/U0	6	0.00	30.94	2746	0	0.00	-----	tdma
0006.5314.81d9	C8/0/0/U0	7	0.00	30.36	2745	0	0.00	-----	tdma
0003.6b1b.ee63	C8/0/0/U0	8	0.00	31.26	2745	0	0.00	-----	tdma
0030.eb15.84e7	C8/0/0/U0	12	0.00	30.36	1157	0	0.00	-----	tdma

For additional information about this or other commands, refer to the following documents on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference*

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

**Secure Socket Layer Server for Usage-Based Billing**

Cisco IOS Release 12.3(17a)BC introduces support for the Secure Socket Layer (SSL) Server, used with the Usage-Based Billing feature of the Cisco CMTS. Usage-Based Billing implements the DOCSIS Subscriber Account Management Interface Specification (SAMIS) format.

This new capability enables the configuration of the SSL server between the Cisco CMTS and a collection server. Configuration, certificate creation, and **debug** commands are added or enhanced to support the SSL Server and certificates with the Usage-Based Billing feature.

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

- *Usage-Based Billing for the Cisco CMTS*

[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_use-bsd\\_bill\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_use-bsd_bill_ps2209_TSD_Products_Configuration_Guide_Chapter.html)

**SSM Mapping**

Cisco IOS Release 12.3(17a)BC introduces Source-Specific Multicast (SSM) Mapping support on the Cisco uBR10012 router.

When the SSM Mapping feature is configured, if a router receives an IGMP version 1 or version 2 membership report for a particular group G, the router translates this in one or more SSM (S, G) channel memberships, such as IGMPv3 (S, G) INCLUDE membership reports) for the well known sources associated with this group.

When the router receives an IGMP version 1 or version 2 membership report for group G, the router uses SSM mapping to determine one or more source IP addresses (Si) for group G. SSM mapping then translates the membership report as an IGMP version 3 report INCLUDE (G, [S1, G], [S2, G]...[Sn, G]) and continues as if it had received an IGMP version 3 report. The router then sends out PIM joins toward (S1, G) to (Sn, G) and continues to be joined to these groups as long as it continues to receive the IGMP version 1 or version 2 membership reports and as long as the SSM mapping for the group remains the same.

When SSM Mapping feature is statically configured on the router, the source address or addresses (S) can be discovered either by a statically configured table on the router or by consulting a DNS. When the statically configured table is changed, or when the DNS mapping changes, the router will leave join to the current sources associated with the joined groups.

For additional information about this feature, refer to the following documents on Cisco.com:

- *Source Specific Multicast (SSM) Mapping*  
[http://www.cisco.com/en/US/docs/ios/12\\_3t/12\\_3t2/feature/guide/gtssmma.html](http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html)

## **New Hardware Features in Cisco IOS Release 12.3(13a)BC6**

There are no new hardware features supported in Cisco IOS Release 12.3(13a)BC6:

## **New Software Features in Cisco IOS Release 12.3(13a)BC6**

There are no new software features supported in Cisco IOS Release 12.3(13a)BC6.

## **New Hardware Features in Cisco IOS Release 12.3(13a)BC5**

There are no new hardware features supported in Cisco IOS Release 12.3(13a)BC5:

## **New Software Features in Cisco IOS Release 12.3(13a)BC5**

There are no new software features supported in Cisco IOS Release 12.3(13a)BC5.

## **New Hardware Features in Cisco IOS Release 12.3(13a)BC4**

There are no new hardware features supported in Cisco IOS Release 12.3(13a)BC4:

## **New Software Features in Cisco IOS Release 12.3(13a)BC4**

There are no new software features supported in Cisco IOS Release 12.3(13a)BC4.

## **New Hardware Features in Cisco IOS Release 12.3(13a)BC3**

There are no new hardware features supported in Cisco IOS Release 12.3(13a)BC3:

## **New Software Features in Cisco IOS Release 12.3(13a)BC3**

There are no new software features supported in Cisco IOS Release 12.3(13a)BC3.

## **New Hardware Features in Cisco IOS Release 12.3(13a)BC2**

There are no new hardware features supported in Cisco IOS Release 12.3(13a)BC2:

## New Software Features in Cisco IOS Release 12.3(13a)BC2

There are no new software features supported in Cisco IOS Release 12.3(13a)BC2.

## New Hardware Features in Cisco IOS Release 12.3(13a)BC1

There are no new hardware features supported in Cisco IOS Release 12.3(13a)BC1.

## New Software Features in Cisco IOS Release 12.3(13a)BC1

There are no new software features supported in Cisco IOS Release 12.3(13a)BC1.

## New Hardware Features in Cisco IOS Release 12.3(13a)BC

The following hardware features are new in Cisco IOS Release 12.3(13a)BC:

- [Cisco Half-Height Gigabit Ethernet Line Card, page 58](#)
- [Processor/IO Memory for the PRE1 Route Processor Module, page 59](#)
- [Cisco uBR10-MC5X20S/U Broadband Processing Engine, page 59](#)
- [Cisco uBR10012 OC-48 DPT/POS Interface Module Support for the Cisco uBR10012 Performance Routing Engine 2 \(PRE2\) Modules, page 60](#)
- [Cisco uBR10012 Performance Routing Engine 2 \(PRE2\) Modules, page 93](#)

### Cisco Half-Height Gigabit Ethernet Line Card

Cisco IOS Release 12.3(13a)BC introduces support for the new Cisco Half-Height Gigabit Ethernet line card (HHGE) for the Cisco uBR10012 router. The HHGE line card is a half-height, single-port, full-bandwidth Gigabit Ethernet line card providing multiple GigE links to the IP backbone. The HHGE line card also supports DOCSIS wideband capability through the Cisco uBR10012 universal broadband router.

The HHGE line card supports IEEE 802.3z-compliant Ethernet interface that can run up to 1 Gbps in full duplex mode. The HHGE line card supports single Ethernet interfaces based on SFP GBIC technology, supporting 1000BASE-SX and 1000BASE-LX/LH physical interfaces with SFP modules. It provides full-duplex 1 Gbps data rate with the PRE-2 performance routing engine module.

The following SFPs are supported by this line card:

- 1000BASE-SX SFP—The SFP-GE-S, 1000BASE-SX SFP operates on ordinary multimode fiber optic link spans of up to 550 meters in length.
- 1000BASE-LX/LH SFP—The SFP-GE-L-SM, 1000BASE-LX/LH SFP operates on ordinary single-mode fiber optic link spans of up to 10,000 meters in length.
- 1000BASE-ZX SFP—The GLC-ZX-SM, 1000BASE-ZX SFP operates on ordinary single-mode fiber optic link spans of up to 70 kilometers (km) in length.

Link spans of up to 100 km are possible using premium single-mode fiber or dispersion-shifted single-mode fiber. The SFP provides an optical link budget of 23 dB—the precise link span length depends on multiple factors such as fiber quality, number of splices, and connectors.

## Restrictions

The HHGE line card cannot be used in slot 1 (subslot 1 or 0), or slot 2 (subslot 1 or 0) in the Cisco uBR10012 universal broadband router.

## Additional Information

For additional information about the Cisco Half-Height Gigabit Ethernet Line Card, refer to the following documents on Cisco.com:

- *Cisco uBR10012 Universal Broadband Router Half-Height Gigabit Ethernet Line Card Installation Quick Start*  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/cable/line\\_cards/ubr\\_hh\\_ge/quick/start/ubr\\_hhge.html](http://www.cisco.com/en/US/docs/interfaces_modules/cable/line_cards/ubr_hh_ge/quick/start/ubr_hhge.html)
- *Upgrading to the Half-Height Gigabit Ethernet Line Card for the Cisco uBR10012 Universal Broadband Router*  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/cable/line\\_cards/ubr\\_hh\\_ge/quick/start/ubr\\_hhge.html](http://www.cisco.com/en/US/docs/interfaces_modules/cable/line_cards/ubr_hh_ge/quick/start/ubr_hhge.html)
- *Configuring the Half-Height Gigabit Ethernet Line Card for the Cisco uBR10012 Universal Broadband Router*  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/cable/line\\_cards/ubr\\_hh\\_ge/configuration/guide/hhgef10.html](http://www.cisco.com/en/US/docs/interfaces_modules/cable/line_cards/ubr_hh_ge/configuration/guide/hhgef10.html)
- *Cisco uBR10012 Universal Broadband Router Hardware Installation Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/guide/u10kspec.html>

## Processor/I/O Memory for the PRE1 Route Processor Module

Cisco IOS Release 12.3(13a)BC introduces support for and availability of additional processor and input/output (I/O) memory for PRE1 route processor modules on the Cisco uBR10012 router.

## Cisco uBR10-MC5X20S/U Broadband Processing Engine

Commencing with Cisco IOS Release 12.3(9a)BC, the Cisco uBR10-MC5X20S/U cable interface line card supports these additional DOCSIS and High Availability features on the Cisco uBR10012 CMTS:

- [PacketCable 1.0 With CALEA](#)
- [Virtual Interface and Frequency Stacking Support on the Cisco uBR10-MC5X20S/U BPE](#)
- [Virtual Interface Support for HCCP N+1 Redundancy](#)

Commencing with Cisco IOS Release 12.3(13a)BC, the Cisco uBR10-MC5X20S/U cable interface line card supports these and additional features:

- [Advanced Spectrum Management Support on the Cisco uBR10012 CMTS](#)
- [Cable Monitor Support for Cisco MC5x20U-D and Cisco MC28U Broadband Processing Engines](#)
- [DOCSIS BPI+ Multiple Root Certificate Support](#)
- [PacketCable Multimedia for the Cisco CMTS](#)
- [Virtual Interface Bundling on the Cisco uBR10-MC5X20S/U BPE](#)

## Cisco uBR10012 OC-48 DPT/POS Interface Module Support for the Cisco uBR10012 Performance Routing Engine 2 (PRE2) Modules

The Cisco uBR10012 OC-48 DPT/POS interface module supports both PRE1 and PRE2 performance routing engine modules in the Cisco uBR10012 router chassis. The Cisco OC-48 DPT/POS interface module is a dual-mode module, providing interface support for Packet over SONET (POS) or Spatial Reuse Protocol (SRP).

For additional information about installing and configuring the Cisco uBR10012 OC-48 DPT/POS interface module, refer to these documents on Cisco.com:

- *Cisco uBR10012 OC-48 DPT/POS Interface Module* (FRU Installation Guide)  
[http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/field\\_replaceable\\_units/ubr\\_oc48.html](http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/field_replaceable_units/ubr_oc48.html)
- *Configuring the Cisco uBR10012 OC-48 DPT/POS Interface Module*  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/cable/line\\_cards/ubr\\_oc48\\_dpt\\_pos/configuration/guide/oc48pre2.html](http://www.cisco.com/en/US/docs/interfaces_modules/cable/line_cards/ubr_oc48_dpt_pos/configuration/guide/oc48pre2.html)

## Cisco uBR10012 Performance Routing Engine 2 (PRE2) Modules

Cisco IOS Release 12.3(9a)BC introduces support for the Cisco uBR10012 performance routing engine 2 (PRE2) route processing modules.

The Cisco uBR10012, which is qualified for PacketCable 1.0, Data over Cable Service Interface Specifications (DOCSIS) 1.1 and EuroDOCSIS 1.1, is built to meet the current and future needs of multiple system operators (MSOs). With full Layer 3 routing capabilities and industry-leading capacity and scalability, the Cisco uBR10012 delivers the highest level of performance for mass deployment of next-generation IP services.

The Cisco uBR10012 is designed to meet the services, performance, and reliability required for large-scale multiservice applications. The Cisco uBR10012 allows cable providers to deliver value-added IP services with consistent high performance. Based on Cisco IOS® Software—the standard in routing technology—the Cisco uBR10012 offers the most advanced networking and routing options available.

The Cisco uBR10012 features these components:

- Eight cable line cards to connect to the cable plant
- Four high-performance WAN interfaces to connect to the IP backbone and external networks
- Two Cisco Timing, Communication, and Control Plus (TCC+) cards to monitor the line cards and power supply
- Two Cisco Performance Routing Engine (PRE) modules with Parallel Express Forwarding (PXF) processors for consistent, high-performance throughput, even with multiple services enabled
- Two Power Entry Modules (PEMs) for uninterrupted power supply

Benefits of the Cisco uBR10012 PRE2 include the following:

- Provides up to 6.2 mpps of processing power in the Cisco uBR10012 router
- Backplane supports up to 6.4 Gbps duplex per slot
- Uses Cisco patented PXF technology to provide maximum IP services performance
- Supports processor redundancy— for enabling 99.999-percent network uptime

- Supports Route Processor Redundancy Plus (RPR+) High Availability functions in the Cisco uBR10012 CMTS headend

Table 4 provides additional details about the features and benefits of the Cisco uBR10012 PRE2.

Features	Benefits
Provides up to 6.2-mpps processing.	The Cisco uBR10012 router with PRE2 provides the IP services and performance that service providers require when deploying new revenue-generating services. In contrast to other CMTS products that support only distributed processing or only centralized processing, the Cisco uBR10012 supports a mix of distributed, centralized, and parallel processing. This ensures optimized performance to a comprehensive suite of line-rate IP services.
Uses Cisco patented PXF technology to provide maximum IP services performance.	PXF technology provides the Cisco uBR10012 router with performance and consistent high throughput, even with multiple, simultaneous services enabled. Using PXF, the Cisco uBR10012 router enables service providers to turn on multiple services without experiencing performance degradation. This is crucial when service providers look to upgrade customers to new types of services. In addition, PXF is a software-based technology that enables the Cisco uBR10012 router to implement new services without upgrading hardware—thereby providing investment protection and saving customers time and money.
Supports processor redundancy—for enabling 99.999-percent network uptime.	Each Cisco uBR10012 chassis supports up to two PRE2 modules for redundancy. The Cisco uBR10012 router is designed to support 99.999-percent uptime and coupled with a superior set of high-availability features and functions.

### Upgrading from Cisco uBR10012 PRE or PRE1 Modules to Cisco uBR10012 PRE2 Modules

For information about insertion, removal and upgrade of Field Replaceable Units such as the PRE2 modules, refer to the following document on Cisco.com:

- *Cisco uBR10012 Universal Broadband Router Performance Routing Engine Module 2*  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/cable/performance\\_routing\\_engine/installation/guide/pre5096.html](http://www.cisco.com/en/US/docs/interfaces_modules/cable/performance_routing_engine/installation/guide/pre5096.html)
- *Cisco Performance Routing Engine (ESR-PRE2) Upgrade Installation*  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/products\\_quick\\_start09186a00802b5eaa.html](http://www.cisco.com/en/US/products/hw/cable/ps2209/products_quick_start09186a00802b5eaa.html)

## New Software Features for Cisco IOS Release 12.3(13a)BC

This section describes the following new software features and CLI command changes for Cisco IOS Release 12.3(13a)BC and the Cisco uBR10012 router:

- Access Control List Support for COPS Intercept
- Admission Control for the Cisco CMTS
- Advanced-mode DOCSIS Set-Top Gateway Issue 1.1
- Advanced Spectrum Management Support on the Cisco uBR10012 CMTS
- Backup Path Testing for the Cisco RF Switch
- Cable Monitor Support for Cisco MC5x20U-D and Cisco MC28U Broadband Processing Engines
- COPS TCP Support for the Cisco Cable Modem Termination System
- DHCP MAC Address Exclusion List for cable-source verify dhcp Command
- DOCSIS 1.0 Concatenation Override
- DOCSIS BPI+ Multiple Root Certificate Support
- Dynamic SID/VRF Mapping Support
- Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems
- High Availability Features:
  - Automatic Revert Feature for HCCP N+1 Redundancy Switchover Events
  - Global N+1 RedundancyShutdown and No Shutdown Enhancement for Cable Interfaces
- MIBs Enhancements
- Multicast QoS Support on the Cisco uBR10012 CMTS
- Online Offline Diagnostics (OOD) Support for the Cisco uBR10012 Universal Broadband Router
- Optional Upstream Scheduler Modes
- PacketCable Emergency 911 Cable Interface Line Card Prioritization
- PacketCable Emergency 911 Services Listing and History
- PacketCable Multimedia for the Cisco CMTS
- Service Independent Intercept (SII) Support
- Transparent LAN Service and Layer 2 Virtual Private Networks
- Virtual Interface Bundling on the Cisco uBR10-MC5X20S/U BPE

## Access Control List Support for COPS Intercept

Cisco IOS Release 12.3(13a)BC introduces enhanced support for Access Control Lists (ACLs) and associated commands for the Common Open Policy Service (COPS) feature.

To configure access control lists (ACLs) for inbound connections to all COPS listener applications on the Cisco CMTS, use the **cops listeners access-list** command in global configuration mode. To remove this setting from the Cisco CMTS, use the **no** form of this command.

```
cops listeners access-list {acl-num | acl-name}
```

```
no cops listeners access-list {acl-num | acl-name}
```

<b>Syntax Description</b>	<i>acl-num</i>	Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.
	<i>acl-name</i>	Numeric identifier that identifies the access list to apply to the current interface. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.

**Note**

When using Access Control Lists (ACLs) with cable monitor and the Cisco uBR10012 router, combine multiple ACLs into one ACL, and then configure cable monitor with the consolidated ACL.

**Additional Information**

Refer also the Service Independent Intercept (SII) feature in this document. For additional information, refer to the following documents on Cisco.com:

- *Configuring COPS for RSVP*, Cisco IOS Versions 12.2 and 12.3  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_cops\\_eng\\_op\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_cops_eng_op_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *Cable Monitor and Intercept Features for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_mon\\_intrcpt\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_mon_intrcpt_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *PacketCable and PacketCable Multimedia on the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_pktcable\\_mm\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *Cisco PacketCable Primer White Paper*  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/products\\_white\\_paper09186a0080179138.shtml](http://www.cisco.com/en/US/products/hw/cable/ps2209/products_white_paper09186a0080179138.shtml)

**Admission Control for the Cisco CMTS**

Cisco IOS Release 12.3(13a)BC introduces Admission Control for the Cisco Cable Modem Termination System (CMTS).

Admission Control for the Cisco Cable Modem Termination System (CMTS) is a multifaceted feature that implements a Quality of Service (QoS) policy on the CMTS Headend. Admission Control establishes efficient resource and bandwidth utilization in a way that was not possible in prior Cisco IOS releases.

Admission Control monitors multiple system-level resources on the Cisco CMTS, and performs automatic resource allocation on a service-request basis. Admission Control maintains optimal system-level operation by preventing resource consumption that would otherwise degrade the performance for the entire Cisco CMTS. Furthermore, Admission Control can allocate upstream or downstream bandwidth resources to specific DOCSIS traffic types, and maintain such prioritization amidst very dynamic traffic conditions.

Admission Control uses two event types for resource monitoring and management—cable modem registration and dynamic service (voice call) requests. When either of these two events occurs on the Cisco CMTS, Admission Control verifies that the associated resources conform to the configured limits prior to admitting and supporting the service call request.

Admission Control is not a mechanism to apply QoS to the traffic flows. Scheduling and queuing are some of the mechanisms used for implementing the QoS. The QoS is applied on a per-packet basis. Admission Control checks are performed before the flow is committed.

Admission Control in Cisco IOS Release 12.3(13)BC monitors the following resources on the Cisco CMTS.

- *CPU utilization*—Admission Control monitors CPU utilization on the Cisco CMTS, and preserves QoS for existing service flows when new traffic would otherwise compromise CPU resources on the Cisco CMTS.
- *Memory resource utilization (I/O, Processor, and combined total)*—Admission Control monitors one or both memory resources and their consumption, and preserves QoS in the same way as CPU utilization.
- *Bandwidth utilization for upstream and downstream*—Admission Control monitors upstream and downstream bandwidth utilization, and associated service classes, whether for data or dynamic service traffic.

Cisco IOS Release 12.3(13a)BC introduces new configuration, **debug** and **show** commands for Admission Control on the Cisco CMTS. For additional information, refer to the following document on Cisco.com:

- *Admission Control for the Cisco Cable Modem Termination System*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_adm.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_adm.html)

## Advanced-mode DOCSIS Set-Top Gateway Issue 1.1

Cisco IOS Release 12.3(13a)BC introduces support for DOCSIS Set-Top Gateway (DSG) Issue 1.1 on the Cisco uBR10012 router. DSG 1.1 builds on and supports the enhancements of DOCSIS Set-Top Gateway Issue 1.0 in the prior Cisco IOS 12.3(9a)BC release.

A-DSG 1.1 introduces powerful support for DOCSIS 1.1 and DOCSIS 2.0, and the latest DOCSIS DSG specifications. The benefits provided by A-DSG include the following:

- Retains the essential nature of out of band (OOB) messaging, but moves it to a modern technology base.
- Replaces single-vendor, low-density, special-purpose equipment on the network, with significantly increased subscriber bandwidth and traffic.
- Consolidates cable modem and STB data traffic on a shared DOCSIS channel.
- Increases high-speed data (HSD) services to cable TV subscribers over the DOCSIS 1.1 infrastructure,
- Extends support for DOCSIS 1.1 digital video broadcast traffic.
- Enables shared or dedicated support for either HSD or video traffic.
- Supports one- or two-way operations, and advanced, two-way interactive applications such as streaming video, Web browsing, e-mail, real-time chat applications, and targeted advertising services.

These powerful advantages maximize the performance and return of hybrid fiber-coaxial (HFC) plant investments.

### Changes from Cisco DSG 1.0

DSG Issue 1.0 is oriented to the DOCSIS DSG-I01 specifications, while DSG Issue 1.1 is oriented towards DOCSIS DSG-I02 specifications, to include the new Advanced Mode DSG (A-DSG).

The following DSG 1.1 features are supported in 12.3(13a)BC while continuing support for Basic Mode DSG:

- DSG 1.1 enables the learning of dynamic tunnel definitions. DSG 1.0 only had static tunnel definitions (programmed into the set-top box).
- DSG 1.1 features new Cisco IOS command-line interface (CLI) configuration and **show** commands for A-DSG configuration and network information.

Unlike earlier issues of DSG, Advanced-mode DSG (A-DSG) uses a DOCSIS MAC Management Message called the Downstream Channel Descriptor (DCD) message, and this DCD message manages the DSG Tunnel traffic. The DCD message is sent once per second on each downstream and is used by the DSG Client to determine which tunnel and classifier to use.

The DCD has a DSG address table located in the DOCSIS MAC management message. The primary difference between DSG 1.0 (and earlier issues) and A-DSG 1.1 is that advanced mode uses DCD messages to manage the DSG tunnels.

The DCD message contains a group of DSG Rules and DSG Classifiers, including the following:

- DSG rules and rule priority
- DSG classifiers
- DSG channel list type/length value (TLV)
- DSG client identifier (whether broadcast, CA System, application, or MAC-level)
- DSG timer list
- DSG upstream channel ID (UCID) list
- Vendor-specific information field

### Prerequisites for DSG 1.1

- Cisco IOS release 12.3(13a)BC or a later 12.3 BC release are required.
- Cisco DSG 1.1 is supported on the Cisco uBR10012 router with PRE1 or PRE2 performance routing engine modules.
- Cisco DSG 1.1 is supported on the Cisco uBR10012 router with the following cable interface line cards and broadband processing engines (BPEs):
  - Cisco uBR10-LCP2-MC16C/MC16E/MC16S Cable Interface Line Card



#### Note

The Cisco uBR10-LCP2-MC16x (C, E, S) cable interface line cards are end of sale. For additional information, refer to END-OF-LIFE NOTICE, NO. 2600 at the following location:

[http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod\\_end-of-life\\_notice0900aecd80183921.html](http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_end-of-life_notice0900aecd80183921.html)

- Cisco uBR10-LCP2-MC28C Cable Interface Line Card
- Cisco uBR10-MC5X20S/U Broadband Processing Engine

## Restrictions and Caveats for DSG 1.1

Cisco DSG 1.1 has the following restrictions:

- Cisco DSG 1.1 does not support Service Flow Quality of Service (QoS), which is available at Layer 3.
- Cisco DSG 1.1 does not support tunnel security, but strictly access control lists (ACLs).
- Cisco DSG 1.1 does not support subinterfaces.
- Cisco DSG 1.1 does not support HCCP N+1 interoperability.
- Cisco DSG 1.1 does not support SNMP MIBS for A-DSG.

## Additional Information about DSG 1.1

- *Advanced-mode DOCSIS Set-Top Gateway Issue 1.1 for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_docsis\\_gw12\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_docsis_gw12_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *DOCSIS Set-Top Gateway (DSG) for the Cisco CMTS*  
[http://www.cisco.com/en/US/products/hw/cable/ps2217/products\\_feature\\_guide09186a00802065c8.html](http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00802065c8.html)
- *Cisco DOCSIS Set-top Gateway White Paper*  
[http://www.cisco.com/en/US/products/hw/cable/ps2217/products\\_white\\_paper09186a00801b3f0f.shtml](http://www.cisco.com/en/US/products/hw/cable/ps2217/products_white_paper09186a00801b3f0f.shtml)
- *CableLabs DOCSIS Set-top Gateway (DSG) Interface Specification SP-DSG-I03-041124*

## Advanced Spectrum Management Support on the Cisco uBR10012 CMTS

Cisco IOS release 12.3(13a)BC introduces Advanced Spectrum Management for the Cisco uBR10012 router, with the following enhancements:

- Supports additional software functionality for the Cisco uBR10-LCP2-MC16C/E/S cable interface line card and the Cisco MC5x20S/U broadband processing engine.



### Note

The Cisco uBR10-LCP2-MC16x (C, E, S) cable interface line cards are end of sale. For additional information, refer to END-OF-LIFE NOTICE, NO. 2600 at the following location:  
[http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod\\_end-of-life\\_notice0900aec80183921.html](http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_end-of-life_notice0900aec80183921.html)

- Supports spectrum analyzer functionality.
- Supports proactive channel management and hopping decisions, so as to avoid the negative impact of ingress noise, and to maintain uninterrupted subscriber service.
- Offers flexible configuration choices, allowing MSOs to determine the priority of the actions to be taken when ingress noise on the upstream channel exceeds the allowable thresholds. The configurable actions are frequency hopping, switching the modulation profile, and reducing the channel width.
- Performs Cisco Network Registrar (CNR) calculations using DSP algorithms in real-time on a per-interface and a per-modem basis.

- Intelligently determines when to modify the frequency, channel width, or modulation profile, based on CNR calculations in the active channel, the number of missed station maintenance polls, and the number of correctable or non-correctable Forward Error Correction (FEC) errors. Previously, channel hopping occurred when the number of missed station maintenance polls exceeded a user-defined threshold or the SNR reported by the Broadcom chip exceeded the DOCSIS thresholds.
- Enhances the Dynamic Upstream Modulation feature for the Cisco uBR-MC16S line card. This feature supports dynamic modulation using two upstream profiles. The primary profile (typically using 16-QAM or a mixed modulation profile) 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.

## Commands for Enhanced Spectrum Management

A variety of commands for enhanced spectrum management now provide new options.

- **cable upstream *n* threshold cnr-profile1 *threshold1-in-dB* cnr-profile2 *threshold2-in-dB* corr-fec *fec-corrected* uncorr-fec *fec-uncorrected***
- **cable upstream *n* upstream threshold snr-profiles *threshold1-in-dB* *threshold2-in-dB***
- **cable upstream *n* threshold corr-fec *corr-fec-threshold***
- **cable upstream *n* threshold uncorr-fec *uncorr-fec-threshold***
- **show cable hop *n* upstream history**
- **show cable hop *n* upstream threshold**



### Note

For additional information and examples, see “Configuring Proactive Channel Management” and “Verifying the Spectrum Management Configuration” in *Spectrum Management for the Cisco CMTS*, at the following URL:

[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_spec.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_spec.html)

For additional information about spectrum management and advanced spectrum management on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Spectrum Management and Advanced Spectrum Management for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_spec.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_spec.html)
- *Advanced Spectrum Management Feature for the Cisco uBR-MC16S Cable Interface Line Card*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_spcrm\\_mgt.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_spcrm_mgt.html)

## Backup Path Testing for the Cisco RF Switch

Cisco IOS Release 12.3(13a)BC introduces the **show hccp channel switch** Cisco IOS command, wherein the Cisco RF Switch communicates with each module in the chassis to provide information as programmed in the RF Switch module bitmap. Cisco IOS Release 12.3(13a)BC performs polling every 10 seconds in response to this command, and reports RF Switch information as stored in cache. In normal operation, the switch requires from two to five seconds for SNMP response.

If SNMP errors are detected in response to this command, the switch may require a significantly longer timeout period. Cisco IOS Release 12.3(13a)BC introduces a keyboard break sequence to disrupt this timeout in such circumstances.

To introduce a break for the **show hccp channel switch** command, use the **Ctrl-Shift-6-x** break sequence—hold **Ctrl-Shift** keys, then press **6** then **x**.

After the break sequence, use the **show hccp g m channel** command to examine each individual HCCP member of a group, as required.

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

- “N+1 Redundancy on the Cisco CMTS” chapter in the *Cisco Cable Modem Termination System Feature Guide*:  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html#wp1043160>
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## Cable Monitor Support for Cisco MC5x20U-D and Cisco MC28U Broadband Processing Engines

Cisco IOS Release 12.3(13a)BC introduces support for the Cable Monitor feature for the Cisco MC5x20U-D broadband processing engine (BPE) and the Cisco MC28U cable interface line card. These field replaceable units (FRUs) apply to the Cisco uBR10012 router, and the latter to the Cisco uBR7246VXR router. This feature enables intercept and monitoring capabilities for DOCSIS-compliant frames.



### Note

The cable monitor feature does not support Access Control Lists (ACLs) for intelligent cable interface line cards such as the Cisco MC28U or Cisco MC16U in the Cisco uBR7246VXR router, or any intelligent cable interface line card in the Cisco uBR10012 router.



### Note

When using ACLs with cable monitor and the Cisco uBR10012 router, combine multiple ACLs into one ACL, and then configure cable monitor with the consolidated ACL.

The Cable Monitor and Intercept features for Cisco Cable Modem Termination System (CMTS) routers provide a software solution for monitoring and intercepting traffic coming from a cable network. This feature also gives service providers Lawful Intercept capabilities, such as those required by the Communications Assistance for Law Enforcement Act (CALEA).

The following example configures cable monitor for a specific interface and the associated MAC addresses:

```
Router(config)# interface Cable3/0
Router(config-if)# cable monitor interface GigabitEthernet0/1
mac-address 000e.5cc8.fa5f
packet-type data ethernet
Router(config-if)#
mac-address 000e.5cac.59f8
packet-type data ethernet
```

To display cable monitor configuration and status information, use the **show interfaces** command in Privileged EXEC mode:

```
Router# show interfaces cable 3/0 monitor
US/ Time Outbound Flow      Flow Type      Flow Packet MAC   MACEncap
DS  Stmp Interface Type      Identifier     Extn. Type  Extn. TypeType
all no   Gi0/1  mac-addr 000e.5cc8.fa5f yes  data  no   -ethernet
all no   Gi0/1  mac-addr 000e.5cac.59f8 yes  data  no   -ethernet
```

To display and monitor traffic statistics and counters over time, use the **show cable modem counters** and the **show interfaces** commands in Privileged EXEC mode, as illustrated:

```
Router# show interfaces cable 3/0 monitor
US/ Time Outbound Flow      Flow Type      Flow Packet MAC      MACEncap
DS Stmp Interface Type      Identifier     Extn. Type     Extn. TypeType
all no      Gi0/1  mac-addr 000e.5cc8.fa5f yes  data  no      -ethernet
all no      Gi0/1  mac-addr 000e.5cac.59f8 yes  data  no      -ethernet
Router# show cable modem 000e.5cac.59f8 counters
MAC Address      US Packets      US Bytes      DS Packets      DS Bytes
000e.5cac.59f8  7537986         3828867645   7199188         3711248288
Router# show interfaces GigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is BCM1250 Internal MAC, address is 000e.d6bd.2001 (bia 000e.d6bd.2001)
  Description: ***Sonde_analyse_trafic***
  Internet address is 82.216.52.1/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/5/0 (size/max/drops/flushes); Total output drops:361
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1094862 packets input, 70425672 bytes, 0 no buffer
    Received 0 broadcasts, 5 runts, 0 giants, 0 throttles
    0 input errors, 10 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 37 multicast, 0 pause input
    0 input packets with dribble condition detected
    188665 packets output, 29355747 bytes, 0 underruns          <<< 188665 packets
    0 output errors, 0 collisions, 6 interface resets
    0 babbles, 0 late collision, 0 deferred
    12 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```

When cable monitor is active, counters for the above commands should increase over time. For additional information about cable monitoring on the Cisco CMTS, refer to these documents on Cisco.com:

- *Cable Monitor and Intercept Features for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cmon.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html)
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## COPS TCP Support for the Cisco Cable Modem Termination System

Cisco IOS Release 12.3(13a)BC introduces optimized support for the Common Open Policy Service (COPS) feature for the Cisco uBR10012 router. This feature supports two new configuration commands for enabling and setting COPS processes. The COPS feature in Cisco 12.3(13a)BC enables the following COPS functions:

### COPS DSCP Marking for the Cisco CMTS

This feature allows you to change the DSCP marking for COPS messages that are transmitted or received by the Cisco router. Differentiated Services Code Point (DSCP) values are used in Quality of Service (QoS) configurations on a Cisco router. DSCP summarizes the relationship between DSCP and IP precedence.

Cisco IOS Release 12.3(13a)BC supports this function with the **cops ip dscp** command in global configuration mode.

### COPS TCP Window Size for the Cisco CMTS

This feature allows you to override the default TCP receive window size that is used by COPS processes. This setting can be used to prevent the COPS server from sending too much data at one time.

Cisco IOS Release 12.3(13a)BC supports this function with the **cops tcp window-size** command in global configuration mode.

**Note**

---

These two commands affect all TCP connections with all COPS servers.

---

## cops ip dscp

To specify the marking for COPS messages that are transmitted by the Cisco router, use the **cops ip dscp** command in global configuration mode. To remove this configuration, use the **no** form of this command.

**cops ip dscp** *x*

**no cops ip dscp**

<b>Syntax Description</b>	x	<p>This value specifies the markings with which COPS messages are transmitted. The following values are supported:</p> <ul style="list-style-type: none"> <li>• 0-63—DSCP value ranging from 0-63.</li> <li>• af11—Use AF11 dscp (001010)</li> <li>• af12—Use AF12 dscp (001100)</li> <li>• af13—Use AF13 dscp (001110)</li> <li>• af21—Use AF21 dscp (010010)</li> <li>• af22—Use AF22 dscp (010100)</li> <li>• af23—Use AF23 dscp (010110)</li> <li>• af31—Use AF31 dscp (011010)</li> <li>• af32—Use AF32 dscp (011100)</li> <li>• af33—Use AF33 dscp (011110)</li> <li>• af41—Use AF41 dscp (100010)</li> <li>• af42—Use AF42 dscp (100100)</li> <li>• af43—Use AF43 dscp (100110)</li> <li>• cs1—Use CS1 dscp (001000) [precedence 1]</li> <li>• cs2—Use CS2 dscp (010000) [precedence 2]</li> <li>• cs3—Use CS3 dscp (011000) [precedence 3]</li> <li>• cs4—Use CS4 dscp (100000) [precedence 4]</li> <li>• cs5—Use CS5 dscp (101000) [precedence 5]</li> <li>• cs6—Use CS6 dscp (110000) [precedence 6]</li> <li>• cs7—Use CS7 dscp (111000) [precedence 7]</li> <li>• default—Use default dscp (000000)</li> <li>• ef—Use EF dscp (101110)</li> </ul>
---------------------------	---	---

**Defaults**

- For messages transmitted by the Cisco router, the default DSCP value is 0.
- For incoming connections to the Cisco router, by default, the COPS engine takes the DSCP value used by the COPS server that initiates the TCP connection.

**Usage Guidelines**

- The **cops ip dscp** command allows the Cisco router to re-mark the COPS packets for either incoming or outbound connections.
- This command affects all TCP connections with all COPS servers.
- This command does not affect existing connections to COPS servers. Once you issue this command, this function is supported only for new connections after that point in time.

**Examples**

The following example illustrates the **cops ip dscp** command with supported command variations:

```
Router(config)# cops ip dscp ?
```

```

<0-63>   DSCP value
af11     Use AF11 dscp (001010)
af12     Use AF12 dscp (001100)
af13     Use AF13 dscp (001110)
af21     Use AF21 dscp (010010)
af22     Use AF22 dscp (010100)
af23     Use AF23 dscp (010110)
af31     Use AF31 dscp (011010)
af32     Use AF32 dscp (011100)
af33     Use AF33 dscp (011110)
af41     Use AF41 dscp (100010)
af42     Use AF42 dscp (100100)
af43     Use AF43 dscp (100110)
cs1      Use CS1  dscp (001000) [precedence 1]
cs2      Use CS2  dscp (010000) [precedence 2]
cs3      Use CS3  dscp (011000) [precedence 3]
cs4      Use CS4  dscp (100000) [precedence 4]
cs5      Use CS5  dscp (101000) [precedence 5]
cs6      Use CS6  dscp (110000) [precedence 6]
cs7      Use CS7  dscp (111000) [precedence 7]
default  Use default dscp (000000)
ef       Use EF   dscp (101110)

```

## Additional COPS Information

Cisco 12.3(13a)BC also supports Access Control Lists (ACLs) for use with COPS. Refer to the [“Access Control List Support for COPS Intercept”](#) section on page 62.

For additional information about configuring COPS on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cable Monitor and Intercept Features for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cmon.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html)
- *Configuring COPS for RSVP*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cops.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cops.html)
- *COPS for RSVP*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cops.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cops.html)

## cops tcp window-size

To override the default TCP receive window size on the Cisco CMTS, use the **cops tcp window-size** command in global configuration mode. This setting allows you to prevent the COPS server from sending too much data at one time. To return the TCP window size to a default setting of 4K, use the **no** form of this command.

**cops tcp window-size** *bytes*

**no cops tcp window-size**

### Syntax Description

<i>bytes</i>	This is the TCP window size setting in bytes. This value can range from 516 to 65535 bytes.
--------------	---

### Defaults

The default COPS TCP window size is 4000 bytes.

**Usage Guidelines**

This command does not affect existing connections to COPS servers. Once you issue this command, this function is supported only for new connections after that point in time.

**Examples**

The following example configures the TCP window size to be 64000 bytes.

```
Router(config)# cops tcp window-size 64000
```

The following example illustrates online help for this command:

```
Router(config)# cops tcp window-size ?
<516-65535> Size in bytes
```

**Additional COPS Information**

Cisco 12.3(13a)BC also supports Access Control Lists (ACLs) for use with COPS. Refer to the [“Access Control List Support for COPS Intercept”](#) section on page 62.

For additional information about configuring COPS on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Cable Monitor and Intercept Features for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cmon.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html)
- *Configuring COPS for RSVP*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cops.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cops.html)
- *COPS for RSVP*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cops.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cops.html)

**DHCP MAC Address Exclusion List for cable-source verify dhcp Command**

Cisco IOS Release 12.3(13a)BC introduces the ability to exclude trusted MAC addresses from standard DHCP source verification checks, as supported in previous Cisco IOS releases for the Cisco CMTS. This feature enables packets from trusted MAC addresses to pass when otherwise packets would be rejected with standard DHCP source verification. This feature overrides the **cable source-verify** command on the Cisco CMTS for the specified MAC address, yet maintains overall support for standard and enabled DHCP source verification processes. This feature is supported on Performance Routing Engine 1 (PRE1) and PRE2 modules on the Cisco uBR10012 router chassis.

To enable packets from trusted source MAC addresses in DHCP, use the **cable trust** command in global configuration mode. To remove a trusted MAC address from the MAC exclusion list, use the **no** form of this command. Removing a MAC address from the exclusion list subjects all packets from that source to standard DHCP source verification.

```
cable trust mac-address
```

```
no cable trust mac-address
```

**Syntax Description**

mac-address	The MAC address of a trusted DHCP source, and from which packets will not be subject to standard DHCP source verification.
-------------	--

**Usage Guidelines**

This command and capability are only supported in circumstances in which the Cable Source Verify feature is first enabled on the Cisco CMTS.

When this feature is enabled in addition to cable source verify, a packet's source must belong to the MAC Exclude list on the Cisco CMTS. If the packet succeeds this exclusionary check, then the source IP address is verified against Address Resolution Protocol (ARP) tables as per normal and previously supported source verification checks. The service ID (SID) and the source IP address of the packet must match those in the ARP host database on the Cisco CMTS. If the packet check succeeds, the packet is allowed to pass. Rejected packets are discarded in either of these two checks.

Any trusted source MAC address in the optional exclusion list may be removed at any time. Removal of a MAC address returns previously trusted packets to non-trusted status, and subjects all packets to standard source verification checks on the Cisco CMTS.

For additional information about the enhanced Cable Source Verify DHCP feature, and general guidelines for its use, refer to the following documents on Cisco.com:

- *IP Address Verification for the Cisco uBR7200 Series Cable Router*  
[http://www.cisco.com/en/US/docs/ios/12\\_0t/12\\_0t7/feature/guide/sourcver.html](http://www.cisco.com/en/US/docs/ios/12_0t/12_0t7/feature/guide/sourcver.html)
- *Filtering Cable DHCP Lease Queries*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/cblsrcvy.html>
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)
- CABLE SECURITY, *Cable Source-Verify and IP Address Security*, White Paper  
[http://www.cisco.com/en/US/tech/tk86/tk803/technologies\\_tech\\_note09186a00800a7828.shtml](http://www.cisco.com/en/US/tech/tk86/tk803/technologies_tech_note09186a00800a7828.shtml)

## DOCSIS 1.0 Concatenation Override

Cisco IOS release 12.3(13a)BC introduces support for the DOCSIS 1.0 concatenation override feature on the Cisco uBR10012 router. This feature provides the ability to disable concatenation on DOCSIS 1.0 cable modems, even in circumstances where concatenation is otherwise supported for the upstream channel.

DOCSIS 1.0 concatenation allows the cable modem to make a single-time slice request for multiple packets, and to send all packets in a single large burst on the upstream. Concatenation was introduced in the upstream receive driver in the previous Cisco IOS releases that supported DOCSIS 1.0+. Per-SID counters were later added in Cisco IOS release 12.1(4)CX for debugging concatenation activity.

In some circumstances, overriding concatenation on DOCSIS 1.0 cable modems may be preferable, and Cisco IOS release 12.3(13a)BC supports either option.



### Note

Even when DOCSIS 1.0 concatenation is disabled with this feature, concatenation remains enabled for cable modems that are compliant with DOCSIS 1.1 or DOCSIS 2.0.

To enable DOCSIS 1.0 concatenation override with Cisco IOS release 12.3(13a)BC and later releases, use the new **docsis10** keyword with the previously supported **cable upstream n concatenation** command in privileged EXEC mode:

```
cable upstream n concatenation docsis10
```

### Syntax Description

<i>n</i>	Specifies the upstream port number. Valid values start with 0 for the first upstream port on the cable interface line card.
----------	---

**Examples**

The following example illustrates DOCSIS 1.0 concatenation override on the Cisco uBR10012 router:

```
Router# no cable upstream 0 concatenation docsis10
```

In this example, DOCSIS 1.0 cable modems are updated with REG-RSP so that they are not permitted to use concatenation.

For additional information about this command, refer to the *Cisco IOS CMTS Cable Command Reference* on Cisco.com:

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

**DOCSIS BPI+ Multiple Root Certificate Support**

Cisco IOS Release 12.3(13a)BC introduces support for multiple DOCSIS root certificates with Baseline Privacy Interface Plus (BPI+) on the Cisco CMTS. This feature enables the Cisco CMTS to support either North American or European cable modems, with the following guidelines for implementation:

- In circumstances in which it is necessary to change from North American root certificates to European root certificates, or vice versa, it is necessary to over write the existing root certificate on the Cisco CMTS, and to reload the Cisco CMTS with the **reload** or **restart** command.
- The Cisco uBR10-MC5X20S/U Broadband Processing Engine (BPE) supports both North American and European root certificates at the same time, and simultaneous root certificate support is a requirement in this case.

**Dynamic SID/VRF Mapping Support**

Cisco IOS release 12.3(13a)BC introduces support for dynamic service ID (SID) and VRF mapping on the Cisco CMTS, to support Voice over IP (VoIP) with MPLS. Formerly, the MPLS SID mapping feature only applied to provisioned service flows. This feature enables the mapping of all PacketCable DQoS service flows to one particular VRF.

For additional information, refer to the following:

- *Mapping Service Flows to MPLS VPN on the Cisco CMTS*

<http://www.cisco.com/en/US/docs/cable/cmts/feature/sfidmpls.html>

**Enhanced Rate Bandwidth Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems**

Cisco IOS release 12.3(13a)BC introduces Enhanced Rate Bandwidth Allocation (ERBA) support for DOCSIS 1.0 cable modems and the Cisco uBR10012 router. ERBA allows DOCSIS1.0 modems to burst their temporary transmission rate up to the full line rate for short durations of time. This capability provides higher bandwidth for instantaneous bandwidth requests, such as those in Internet downloads, without having to make changes to existing service levels in the QoS Profile.

This feature enables MSOs to set the DOCSIS 1.0 cable modems burst transmissions, with mapping to overriding DOCSIS 1.1 QoS profile parameters on the Cisco CMTS. DOCSIS 1.0 cable modems require DOCSIS 1.0 parameters when registering to a matching QoS profile. This feature enables maximum downstream line rates, and the ERBA setting applies to all cable modems that register to the corresponding QoS profile.

**Note**

QoS definitions must previously exist on the Cisco CMTS headend to support this feature.

ERBA for DOCSIS 1.0 cable modems is supported with these new or enhanced commands or keywords in Cisco IOS release 12.3(13a)BC:

- `cable qos pro max-ds-burst burst-size`
- `show cable qos profile n [verbose]`

To define ERBA on the downstream for DOCSIS 1.0 cable modems, use the **`cable qos promax-ds-burst`** command in global configuration mode. To remove this ERBA setting from the QoS profile, use the **`no`** form of this command.

```
cable qos pro max-ds-burst burst-size
```

```
no cable qos pro max-ds-burst
```

---

### Syntax Description

<code>burst-size</code>	The QoS profile's downstream burst size in bytes.
-------------------------	---

---

To display ERBA settings as applied to DOCSIS 1.0 cable modems and QoS profiles on the Cisco CMTS, use the **`show cable qos profile`** command in Privileged EXEC mode.

The following example of the **`cable qos profile`** command in global configuration mode illustrates changes to the **`cable qos profile`** command. Fields relating to the ERBA feature are shown in bold for illustration:

```
Router(config)# cable qos pro 10 ?
  grant-interval      Grant interval
  grant-size          Grant size
  guaranteed-upstream  Guaranteed Upstream
  max-burst           Max Upstream Tx Burst
  max-ds-burst       Max Downstream Tx burst (cisco specific)
  max-downstream   Max Downstream
  max-upstream        Max Upstream
  name                QoS Profile name string (cisco specific)
  priority            Priority
  privacy             Cable Baseline Privacy Enable
  tos-overwrite       Overwrite TOS byte by setting mask bits to value
```

The following example of the **show cable qos profile** command illustrates that the maximum downstream burst has been defined, and is a management-created QoS profile:

```
Router# show cable qos pro
ID  Prio Max      Guarantee Max      Max      TOS  TOS   Create  B      IP prec.
      upstream upstream downstream Max      TOS  TOS   Create  B      IP prec.
      bandwidth bandwidth bandwidth tx      mask value by      priv rate
1    0    0          0          0        0     0xFF 0x0    cmts(r) no   no
2    0    64000     0          1000000  0     0xFF 0x0    cmts(r) no   no
3    7    31200     31200     0        0     0xFF 0x0    cmts     yes  no
4    7    87200     87200     0        0     0xFF 0x0    cmts     yes  no
6    1    90000     0          90000    1522 0xFF 0x0    mgmt    yes  no
10   1    90000     0          90000    1522 0x1  0xA0  mgmt    no   no
50   0    0          0          96000    0     0xFF 0x0    mgmt     no   no
51   0    0          0          97000    0     0xFF 0x0    mgmt     no   no
```

The following example illustrates the maximum downstream burst size in sample QoS profile 10 with the **show cable qos prof verbose** command in privileged EXEC mode:

```
Router# show cable qos pro 10 ver
Profile Index          10
Name
Upstream Traffic Priority      1
Upstream Maximum Rate (bps)   90000
Upstream Guaranteed Rate (bps) 0
Unsolicited Grant Size (bytes) 0
Unsolicited Grant Interval (usecs) 0
Upstream Maximum Transmit Burst (bytes) 1522
Downstream Maximum Transmit Burst (bytes) 100000
IP Type of Service Overwrite Mask 0x1
IP Type of Service Overwrite Value 0xA0
Downstream Maximum Rate (bps)   90000
Created By                  mgmt
Baseline Privacy Enabled     no
```

## Usage Guidelines

If a cable modem registers with a QoS profile that matches one of the existing QoS profiles on the Cisco CMTS, then the maximum downstream burst size, as defined for that profile, is used instead of the default DOCSIS QoS profile of 1522.

For example, a DOCSIS 1.0 configuration that matches QoS profile 10 in the previous examples would be as follows:

```
03 (Net Access Control)      = 1
04 (Class of Service Encodings Block)
  S01 (Class ID)             = 1
  S02 (Maximum DS rate)      = 90000
  S03 (Maximum US rate)      = 90000
  S06 (US burst)             = 1522
  S04 (US Channel Priority)   = 1
  S07 (Privacy Enable)       = 0
```

The maximum downstream burst size (as well as the ToS overwrite values) are not explicitly defined in the QoS configuration file because they are not defined in DOCSIS. However, because all other parameters are a perfect match to profile 10 in this example, then any cable modem that registers with these QoS parameters has a maximum downstream burst of 100000 bytes applied to it.

For further illustration, consider a scenario in which packets are set in lengths of 1000 bytes at 100 packets per second (pps). Therefore, the total rate is a multiplied total of 1000, 100, and 8, or 800kbps.

To change these settings, two or more traffic profiles are defined, with differing downstream QoS settings as desired. Table 3 provides two examples of such QoS profiles for illustration:

**Table 3** *Sample QoS Profiles with Differing ERBA (Maximum Downstream) Settings*

QoS Profile Setting	QoS Profile 101	QoS Profile 102
Maximum Downstream Transmit Burst (bytes)	max-burst 4000	max-burst 4000
Maximum Downstream Burst (bps)	max-ds-burst 20000	max-ds-burst 5000
Maximum Downstream Bandwidth	max-downstream 100	max-downstream 100

In this scenario, both QoS profiles are identical except for the max-ds-burst size, which is set to 5000 in QoS profile 101 and 5000 in QoS profile 102.

### Optimal Settings for ERBA

DOCSIS allows the setting different token bucket parameters for each service flow, including the token bucket burst size. When burst sizes are closer to 0, QoS is enforced in a stricter manner, allowing a more predictable sharing of network resources, and as a result easier network planning.

When burst sizes are larger, individual flows can transmit information faster (lower latency), although the latency variance can be larger as well.

For individual flows, a larger burst size is likely to be better. As long as the system is not congested, a large burst size reduces the chances of two flows transmitting at the same time, because each burst is likely to take less time to transmit. However, as channel bandwidth consumption increases, it is probably that large burst traffic would exceed the thresholds of buffer depths, and latency is longer than with well shaped traffic.

For additional information about the **cable qos profile** command and configuring QoS profiles, refer to the following documents on Cisco.com:

- *Cisco Broadband Cable Command Reference Guide*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)
- *Configuring DOCSIS 1.1 on the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_docs.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html)

## High Availability Features

Cisco IOS release 12.3(13a)BC introduces several High Availability features on the Cisco uBR10012 router:

- [Automatic Revert Feature for HCCP N+1 Redundancy Switchover Events, page 78](#)
- [Global N+1 Redundancy, page 79](#)
- [PacketCable Emergency 911 Cable Interface Line Card Prioritization, page 82](#)
- [PacketCable Emergency 911 Services Listing and History, page 82](#)
- [Shutdown and No Shutdown Enhancement for Cable Interfaces, page 79](#)

### Automatic Revert Feature for HCCP N+1 Redundancy Switchover Events

Cisco IOS release 12.3(13a)BC introduces the Auto-Revert feature for the Cisco uBR10012 router, to further enhance HCCP N+1 Redundancy on the Cisco CMTS. With this feature, when a switchover event is performed in manual fashion, from the HCCP Protect line card, and the Protect line card has a

hardware fault, HCCP automatically reverts back to the HCCP Working line card. This is a very helpful feature, in that periodic switchovers can be performed for regular maintenance or testing purposes, yet subscriber service is not interrupted should such switchovers reveal unexpected problems with HCCP Protect line cards.

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

- “N+1 Redundancy for the Cisco Cable Modem Termination System,” *Cisco CMTS Feature Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html>
- *Cisco Broadband Cable Command Reference Guide*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## Global N+1 Redundancy

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

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

- “N+1 Redundancy for the Cisco Cable Modem Termination System,” *Cisco CMTS Feature Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html>
- *Cisco Broadband Cable Command Reference Guide*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## Shutdown and No Shutdown Enhancement for Cable Interfaces

Cisco IOS release 12.3(13a)BC introduces a new behavior with the **[no] shutdown interface** configuration command. In HCCP N+1 Redundancy schemes, an interface that is shut down with the shutdown command does not create an HCCP Switchover event for the associated Working or Protect interface. Instead, cable modems go offline and return online when the **no shutdown** command is issued.

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

- “N+1 Redundancy for the Cisco Cable Modem Termination System,” *Cisco CMTS Feature Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/uFGnpls1.html>
- *Cisco Broadband Cable Command Reference Guide*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## MIBs Enhancements

### Subinterface support in ifTable Object

Cisco IOS Release 12.3(13a)BC introduces enhanced SNMP MIB support in which subinterface information is included in the ifTable for the associated device. This enhanced ifTable provides new subinterface information in addition to the main interface information previously supported in earlier Cisco IOS releases.

This subinterface MIB information is only supported in the ifTable if an IP address is assigned to the subinterface and the main interface under which it resides. This subinterface MIB information is not supported when the IP address of a main or subinterface is removed with the **no interface** command in interface configuration mode.

For additional information about the ifTable and SNMP MIBs for the Cisco CMTS, refer to the following document on Cisco.com:

- *Cisco CMTS MIB Specifications Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html>

## Multicast QoS Support on the Cisco uBR10012 CMTS

Cisco IOS Release 12.3(13a)BC introduces support for Multicast downstream QoS feature. This feature provides the ability to assign static mapping to a multicast group. The Multicast downstream QoS feature uses the existing infrastructure (DOCSIS 1.1 service flow) to assign a multicast service identifier (SID) to a multicast group used in the Baseline Privacy Interface (BPI) encryption feature.

When disabled, the Multicast downstream QoS feature does not impact any other features. The multicast packets to downstream cable interfaces are sent to the default service flow.

This feature is being implemented in response to CSCeg22989 which states, multicast traffic is not classified to any service flow, and therefore ends up queued on the default service flow. The default service flow has no specific QoS guarantees assigned to it. So once the interface approaches congestion level, multicast packets may be dropped.

### Restrictions

- The multicast definitions are per-bundle, not per interface. This means that all downstreams in a bundle share the same multicast to QoS association. The downstreams will create their own service flows according to the same QoS parameters.
- Multicast to QoS definitions can not be assigned per sub-interface
- Multicast SIDs are not deleted when a group becomes idle (no response to IGMP reports).
- The QoS assignments for a multicast group can not be changed dynamically. If the user wishes to change them then a new “cable match” command must be configured.
- Multicast QoS is not supported with Multicast Echo on the Cisco uBR10012 router. Multicast; however, MultiCast Echo is supported on the Cisco uBR10012 for packets that go through multicast forwarding (arrive to the router on a WAN interface).

### New and Changed Commands

#### **cable match address**

Use the existing “cable match” command to assign QoS to a multicast group, with BPI either enabled or disabled.

```
Router# cable match address <number>|<name> [service-class <name> [bpi-enable]]
Router# no cable match address [<number>|<name> [service-class <name> [bpi-enable]]]
```

#### **debug cable mcast-qos**

Use this command to turn on CMTS Multicast QoS debugging.

```
Router# debug cable mcast-qos
```

## Online Offline Diagnostics (OOD) Support for the Cisco uBR10012 Universal Broadband Router

Cisco IOS Release 12.3(13a)BC introduces support for Online Offline Diagnostics (OOD) in the field for the Cisco uBR1002 router, including support in a high availability environment with HCCP N+1 Redundancy. The Online Offline Diagnostics (OOD) feature introduces a Field Diagnostic tool that provides a method of testing and verifying line card hardware problems.

This feature is supported on the following field replaceable units (FRUs) of the Cisco uBR10012 router:

- Cisco uBR10012 PRE1 and PRE2 Performance Routing Engine (PRE1 and PRE2) modules
- Cisco uBR10K-MC520S/U broadband processing engine (BPE)
- Cisco uBR10012 OC-48 DPT/POS WAN interface module

To view a list of hardware on the Cisco uBR10012 router that is supported by Field Diagnostics, refer to the following document:

- *Online Offline Diagnostics - Field Diagnostics on Cisco uBR10012 Router User's Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/troubleshooting/fdub10k.html>

If you would like to perform a hardware diagnostic test on a line card in your Cisco uBR10000 series router, an OOD Field Diagnostic image can be downloaded free of charge from Cisco Systems and used to test whether the line card problems are indeed due to faulty hardware. The test results verify whether or not the hardware is faulty.

## Optional Upstream Scheduler Modes

With this feature, the user is able to select either Unsolicited Grant Services (UGS) or Real Time Polling Service (rtPS) scheduling types, as well as packet-based or TDM-based scheduling. Low latency queueing (LLQ) emulates a packet-mode-like operation over the Time Division Multiplex (TDM) infrastructure of DOCSIS. As such, the feature provides the typical tradeoff between packets and TDM: with LLQ, the user has more flexibility in defining service parameters for UGS or rtPS, but with no guarantee (other than statistical distribution) regarding parameters such as delay and jitter.

### Restrictions

- To ensure proper operation, Call Admission Control (CAC) must be enabled. When the Low Latency Queueing (LLQ) option is enabled, it is possible for the upstream path to be filled with so many calls that it becomes unusable, making voice quality unacceptable. CAC must be used to limit the number of calls to ensure acceptable voice quality, as well as to ensure traffic other than voice traffic.
- Even if CAC is not enabled, the default (DOCSIS) scheduling mode blocks traffic after a certain number of calls.
- Unsolicited Grant Services with Activity Detection (UGS-AD) and Non Real Time Polling Service (nrtPS) are not supported.

### New and Changed Commands

#### **cable upstream *n* scheduling type**

Use this new command to turn the various scheduling modes on or off, where *n* specifies the upstream port.

```
Router(config-if)# [no] cable upstream n scheduling type [ugs | rtps] mode [llq | docsis]
```

For additional information about scheduler enhancements on the Cisco CMTS, refer to the following:

- *Cisco CMTS Feature Guide — Configuring Upstream Scheduler Modes on the Cisco CMTS*

<http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/cmtsfg.html>

- *DOCSIS 1.1 for the Cisco CMTS*

[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_docs.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html)

## PacketCable Emergency 911 Cable Interface Line Card Prioritization

Cisco IOS Release 12.3(13a)BC introduces PacketCable Emergency 911 cable interface line card prioritization on the Cisco CMTS. This feature enables cable interface line cards that are supporting an Emergency 911 call to be given automatic priority over cable interface line cards supporting non-emergency voice calls, even in the case of HCCP switchover events. In such cases, Protect HCCP line card interfaces automatically prioritize service to Emergency 911 voice calls, should Working HCCP cable interface line cards be disrupted. This feature is enabled by default in Cisco IOS release 12.3(13a)BC, and may not be disabled with manual configuration.



**Note**

---

Emergency 911 cable interface line card prioritization applies only to PacketCable voice calls.

---

During HCCP switchover events, cable modems recover in the following sequence in Cisco IOS release 12.3(13a)BC:

1. Cable modems supporting Emergency 911 voice traffic
2. Cable modems supporting non-emergency voice traffic
3. Cable modems that are nearing a T4 timeout event, in which service would be disrupted
4. Remaining cable modems

To view information about Emergency 911 voice events and cable interface line card prioritization on the Cisco CMTS, use the **show hccp <int x> <int y> modem** and **show hccp event-history** commands in privileged EXEC mode.

- *PacketCable and PacketCable Multimedia on the Cisco CMTS*

[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_pkcb.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html)

- *Cisco PacketCable Primer White Paper*

[http://www.cisco.com/en/US/products/hw/cable/ps2209/products\\_white\\_paper09186a0080179138.shtml](http://www.cisco.com/en/US/products/hw/cable/ps2209/products_white_paper09186a0080179138.shtml)

## PacketCable Emergency 911 Services Listing and History

Cisco IOS release 12.3(13a)BC introduces enhanced informational support for PacketCable Emergency 911 calls on the Cisco CMTS, to include the following information and related history:

- active Emergency 911 calls
- recent Emergency 911 calls
- regular voice calls
- voice calls made after recent Emergency 911 calls

This feature is enabled and supported with the following new Cisco IOS command-line interface (CLI) configuration and **show** commands:

- **cable high-priority-call-window <minutes>**
- **show cable calls [ interface cx/y | slot z ]**

- **show cable calls** [*interface* | *slot*] for the Cisco uBR 7200 Series
- **show cable calls** [*interface* | *slot/subslot*] for the Cisco uBR10012 router
- **show cable modem** [*ip\_addr* | *mac\_addr* | *interface*] **calls**

To set the call window (in minutes) during which the Cisco CMTS maintains records of Emergency 911 calls, use the **cable high-priority-call-window** command in global configuration mode. To remove the call window configuration from the Cisco CMTS, use the no form of this command:

```
cable high-priority-call-window <minutes>
no cable high-priority-call-window
```

The following command example configures the call window on the Cisco uBR10012 router to be 1 minute in length:

```
Router(config)# cable high-priority-call-window 1
```

To observe Emergency 911 calls made within the configured window, use the **show cable calls** command in privileged EXEC mode:

```
show cable calls
```

The following command example illustrates that one Emergency 911 call was made on the Cable8/1/1 interface on the Cisco uBR10012 router during the window set for high priority calls:

```
Router# show cable calls
Interface  ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCms  RecentHiPriCms
Cable5/0/0  0                  0                0                  0
Cable5/0/1  0                  0                0                  0
Cable5/1/0  0                  0                0                  0
Cable5/1/1  0                  0                0                  0
Cable5/1/2  0                  0                0                  0
Cable5/1/3  0                  0                0                  0
Cable5/1/4  0                  0                0                  0
Cable6/0/0  0                  0                0                  0
Cable6/0/1  0                  0                0                  0
Cable7/0/0  0                  0                0                  0
Cable7/0/1  0                  0                0                  0
Cable8/1/0  0                  0                0                  0
Cable8/1/1  1                  1                0                  0
Cable8/1/2  0                  0                0                  0
Cable8/1/3  0                  0                0                  0
Cable8/1/4  0                  0                0                  0
Total      1                  1                0                  0
```

The following command example illustrates the change on the Cisco uBR10012 router when this Emergency 911 calls ends:

```
Router# show cable calls
Interface  ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCms  RecentHiPriCms
Cable5/0/0  0                  0                0                  0
Cable5/0/1  0                  0                0                  0
Cable5/1/0  0                  0                0                  0
Cable5/1/1  0                  0                0                  0
Cable5/1/2  0                  0                0                  0
Cable5/1/3  0                  0                0                  0
Cable5/1/4  0                  0                0                  0
Cable6/0/0  0                  0                0                  0
Cable6/0/1  0                  0                0                  0
Cable7/0/0  0                  0                0                  0
Cable7/0/1  0                  0                0                  0
Cable8/1/0  0                  0                0                  0
Cable8/1/1  0                  0                0                  1
Cable8/1/2  0                  0                0                  0
Cable8/1/3  0                  0                0                  0
```

```

Cable8/1/4 0          0          0          0
Total      0          0          0          1

```

The following command example illustrates available information when making a voice call from the same MTA to another MTA on the same interface:

```

Router# show cable calls
Interface  ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
Cable5/0/0 0                0                0                0
Cable5/0/1 0                0                0                0
Cable5/1/0 0                0                0                0
Cable5/1/1 0                0                0                0
Cable5/1/2 0                0                0                0
Cable5/1/3 0                0                0                0
Cable5/1/4 0                0                0                0
Cable6/0/0 0                0                0                0
Cable6/0/1 0                0                0                0
Cable7/0/0 0                0                0                0
Cable7/0/1 0                0                0                0
Cable8/1/0 0                0                0                0
Cable8/1/1 0                2                1                1
Cable8/1/2 0                0                0                0
Cable8/1/3 0                0                0                0
Cable8/1/4 0                0                0                0
Total      0                2                1                1

```

The following command example illustrates available information when a voice call from the same MTA to another MTA on the same interface ends:

```
Router# show cable calls
Interface  ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
Cable5/0/0  0                  0                0                  0
Cable5/0/1  0                  0                0                  0
Cable5/1/0  0                  0                0                  0
Cable5/1/1  0                  0                0                  0
Cable5/1/2  0                  0                0                  0
Cable5/1/3  0                  0                0                  0
Cable5/1/4  0                  0                0                  0
Cable6/0/0  0                  0                0                  0
Cable6/0/1  0                  0                0                  0
Cable7/0/0  0                  0                0                  0
Cable7/0/1  0                  0                0                  0
Cable8/1/0  0                  0                0                  0
Cable8/1/1  0                  0                0                  1
Cable8/1/2  0                  0                0                  0
Cable8/1/3  0                  0                0                  0
Cable8/1/4  0                  0                0                  0
Total      0                  0                0                  1
```

The following example illustrates the **show cable modem calls** command on the Cisco uBR10012 router over a period of time, with changing call status information:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address   IP Address   I/F   Prim  CMCallStatus  LatestHiPriCall
              (min:sec)
0000.cab7.7b04 10.10.155.38 C8/1/1/U0 18   R        0:39
```

The following example illustrates that call information disappears when a call ends:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address   IP Address   I/F   Prim  CMCallStatus  LatestHiPriCall
              (min:sec)
```

The following example illustrates a new Emergency 911 call on the Cisco CMTS:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address   IP Address   I/F   Prim  CMCallStatus  LatestHiPriCall
              (min:sec)
0000.cab7.7b04 10.10.155.38 C8/1/1/U0 18   HV       1:30
```

The following example illustrates a the end of the Emergency 911 call on the Cisco CMTS:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address   IP Address   I/F   Prim  CMCallStatus  LatestHiPriCall
              (min:sec)
0000.cab7.7b04 10.10.155.38 C8/1/1/U0 18   R        0:3
```

The following example illustrates a non-emergency voice call on the Cisco CMTS from the same MTA:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address      IP Address      I/F      Prim  CMCallStatus  LatestHiPriCall
                               Sid                               (min:sec)
0000.ca36.f97d  10.10.155.25   C8/1/1/U0 5     V      -
0000.cab7.7b04  10.10.155.38   C8/1/1/U0 18    RV     0:30
```

The following example illustrates the end of the non-emergency voice call on the Cisco CMTS:

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address      IP Address      I/F      Prim  CMCallStatus  LatestHiPriCall
                               Sid                               (min:sec)
0000.cab7.7b04  10.10.155.38   C8/1/1/U0 18    R      0:36
```

For additional information about PacketCable Emergency 911 calls on the Cisco CMTS, refer to the following documents on Cisco.com:

- *PacketCable and PacketCable Multimedia on the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_pkcb.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html)
- *Cisco PacketCable Primer White Paper*  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/products\\_white\\_paper09186a0080179138.shtml](http://www.cisco.com/en/US/products/hw/cable/ps2209/products_white_paper09186a0080179138.shtml)

## PacketCable Multimedia for the Cisco CMTS

Cisco IOS Release 12.3(13a)BC introduces support for PacketCable Multimedia (PCMM) on the Cisco uBR10012 universal broadband router, and fully supports the CableLabs *PacketCable Multimedia Specification*, PKT-SP-MM-I02-040930.

<http://www.cablelabs.com/packetcable/specifications/multimedia.html>

As described by CableLabs, some key features of the PCMM service delivery framework include the following:

- Simple, powerful access to DOCSIS 1.1 QoS mechanisms supporting both time and volume-based network resource authorizations
- Abstract, event-based network resource auditing and management mechanisms
- A robust security infrastructure that provides integrity and appropriate levels of protection across all interfaces

More specifically, Cisco IOS Release 12.3(13a)BC expands or changes several PacketCable functions in earlier Cisco IOS releases, including the following:

- **Additional COPS Decision Messages**—PCMM supports additional COPS decision messages, such as the following. The new objects for messages, such as Gate-Set, Gate-Set-Ack and Gate-Info, include different traffic profile definitions, different gate object formats, with additional objects for gate state reporting and flow utilization.
  - Gate-Set
  - Gate-Set-Ack
  - Gate-Set-Err

- Gate-Info
  - Gate-Info-Ack
  - Gate-Info-Err
  - Gate-Delete
  - Gate-Delete-Ack
  - Gate-Delete-Err
  - State-Report
- **Different COPS client and UDP port for COPS sessions**—PCMM uses a different COPS client type than does basic PacketCable, and PCMM uses a different UDP port for its COPS sessions. This can help to distinguish between PacketCable and PCMM COPS sessions on the Cisco CMTS.
  - **MultiMedia State Machine**—PCMM supports a different MultiMedia state machine than does PacketCable. The following are machine state changes introduced in PCMM with Cisco IOS Release 12.3(13a)BC:
    - PCMM gates are all unidirectional. In PacketCable, each gate is associated with both an upstream and downstream service flow. Although unidirectional flows are allowed, a bidirectional phone connection only has one gate.  
 PCMM differs in that each gate is now unidirectional, and is associated with only one service flow. As a result, the gate info element structure in PCMM differs significantly from that of PacketCable. PCMM only needs to maintain one set of service flow information, rather than maintaining both upstream and downstream information as does PacketCable.
    - DOCSIS DSX service flow information is now maintained on the Cisco CMTS. With PacketCable, gates are authorized, reserved, or committed first on the Cisco CMTS with a specific gate ID, and then the Cisco CMTS initiates a DSX exchange using the reserved or committed gate ID in the message. With PacketCable, the cable modem must issue the DSX message and create the service flows. However, with PCMM, when a gate is reserved or committed, the DSX message is generated and sent immediately by the Cisco CMTS. Therefore, the Policy Server sends all of the service flow information necessary to setup the service flow to the Cisco CMTS instead of the cable modem. This causes a major change in the state machine that controls the gate allocation procedures.
    - New timer definitions and event actions are supported on PCMM. New timer definitions and timer event actions are supported for proper behavior of the net state machine. Some of the timers used with PacketCable have been eliminated, while the events associated with other times have changed for PCMM.
    - New state transitions that did not exist in PacketCable 1.x have been added to PCMM. Specifically, a gate can now be transitioned back from Committed to Authorized or Reserved state.
    - Cable interface line cards and broadband processing engines perform distributed DOCSIS functions. The Cisco MC28U cable interface line card on the Cisco uBR7200 series routers, and all the line cards on the Cisco uBR10012 router, are considered distributed, because the DOCSIS functionality is performed by the line card processor. The GCP signaling for PCMM and the gate state machine will be executed on the NPE or RP processor. Because of the split in this functionality, IPC signaling resides between the gate state machine and the DOCSIS layer processing.
  - **Event management**—Event management messages have been modified to include information on the modified traffic profiles, and to match changes in the PCMM state machine. In addition, objects have been added to help support Gate usage and Gate commit time objects, used for usage limit based and time based gates.

For additional information about PacketCable and PacketCable Multimedia on the Cisco CMTS, refer to the following documents on Cisco.com:

- *PacketCable and PacketCable Multimedia on the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_pkcb.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html)
- *Cisco PacketCable Primer White Paper*  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/products\\_white\\_paper09186a0080179138.shtml](http://www.cisco.com/en/US/products/hw/cable/ps2209/products_white_paper09186a0080179138.shtml)

“PacketCable is a CableLabs®-led initiative that is aimed at developing interoperable interface specifications for delivering advanced, real-time multimedia services over two-way cable plant. Built on top of the industry's highly successful cable modem infrastructure, PacketCable networks use Internet protocol (IP) technology to enable a wide range of multimedia services, such as IP telephony, multimedia conferencing, interactive gaming, and general multimedia applications.” (PacketCable.com)

CableLabs® describes key features of the PacketCable Multimedia IP service delivery framework as follows:

- Simple, powerful access to DOCSIS® 1.1 QoS mechanisms supporting both time and volume-based network resource authorizations
- Abstract, event-based network resource auditing and management mechanisms
- A robust security infrastructure that provides integrity and appropriate levels of protection across all interfaces

PacketCable™ is a registered trademark of CableLabs®. Additional information and specifications are available online at the following CableLabs websites:

- PacketCable website  
<http://www.cablelabs.com/packetcable/>
- PacketCable Multimedia specifications  
<http://www.cablelabs.com/packetcable/specifications/multimedia.html>

## Service Independent Intercept (SII) Support

Cisco CMTS supports the Communications Assistance for Law Enforcement Act (CALEA) for voice and data. Cisco IOS Release 12.3(13a)BC introduces support for Service Independent Intercept (SII) on the Cisco uBR10012 CMTS. Cisco SII provides a more robust level of the lawful intercept (LI) options offered in the Packet Intercept feature. Cisco SII is the next level of support for judicially authorized electronic intercept, to include dial access, mobile wireless, tunneled traffic, and Resilient Transport Protocol (RTP) for voice and data traffic on the Cisco CMTS. SII on the Cisco CMTS includes these functions:

- Packet intercept on specified or unspecified interfaces or ports
- Packet intercept on virtual interface bundles
- Corresponding SNMP MIB enhancements for each of these functions, as intercept requests are initiated by a mediation device (MD) using SNMPv3

**Note**

At the time of publication, the Cisco IOS 12.3 BC release train does not support virtual private networks with the SII feature. The CISCO-TAP-MIB does not specify any particular VPN, so this MIB is not assigned to a particular instance of VPN routing/forwarding (VRF). For restrictions on this platform, see “[Overview of CISCO-TAP-MIB](#)” in *Cable Monitor and Intercept Features for the Cisco CMTS*. See [Additional Information, page 89](#).

**Note**

No new CLI commands are provided for this feature in Cisco IOS Release 12.3(13a)BC.

Cisco IOS Release 12.3(13a)BC enables full Multiple Service Operator (MSO) compliance with SII and LI regulations. Service providers worldwide are legally required to allow government agencies to conduct surveillance on the service provider's traditional telephony equipment. The objective of the SII feature is to enable service providers with New World networks that legally allow government agencies to conduct electronic network surveillance.

Lawful Intercept (LI) describes the process and judicial authority by which law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications. LI is authorized by judicial or administrative order and implemented for either voice or data traffic on the Cisco CMTS. [Table 4](#) lists the differences between packet intercept and SII features as implemented on the Cisco uBR10012.

**Table 4** Differences Between Packet Intercept and SII Features on the Cisco uBR10012

Feature	Packet Intercept	Service Independent Intercept
Interface Type	Cable	Cable
IP Masks	255.255.255.255 or 0.0.0.0	255.255.255.255 or 0.0.0.0
L4 Ports	Any single port or 0–65535	Any single port or 0–65535
Protocol	UDP	Any
TOS/DSCP	Not supported	Supported

## Additional Information

For additional information, refer to the following documents:

- *Configuring COPS for RSVP*, Cisco IOS Versions 12.2 and 12.3  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cops.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cops.html)
- *Cable Monitor and Intercept Features for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cmon.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html)
- *PacketCable and PacketCable Multimedia on the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html>
- *Cisco PacketCable Primer White Paper*  
[http://www.cisco.com/en/US/products/hw/cable/ps2209/products\\_white\\_paper09186a0080179138.shtml](http://www.cisco.com/en/US/products/hw/cable/ps2209/products_white_paper09186a0080179138.shtml)

## Transparent LAN Service and Layer 2 Virtual Private Networks

Cisco IOS Release 12.3(13a)BC introduces the following changes or requirements for the TLS feature with Layer 2 VPNs:

- When the TLS feature is used with Layer 2 VPNs, the participating cable modems must have the Baseline Privacy Interface security feature (BPI) enabled. Otherwise, the Cisco CMTS drops such Layer 2 traffic in the upstream or downstream.
- Information about customer premises equipment (CPE) does not display in the output of the **show cable modem** command.

Refer to the following documents on Cisco.com for additional TLS information:

- *TLS for the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/tls-cmts.html>
- *TLS Over Cable* - TAC Document #60027  
[http://www.cisco.com/en/US/products/hw/cable/ps2217/products\\_configuration\\_example09186a08029160d.shtml](http://www.cisco.com/en/US/products/hw/cable/ps2217/products_configuration_example09186a08029160d.shtml)

## Virtual Interface Bundling on the Cisco uBR10-MC5X20S/U BPE

Cisco IOS Release 12.3(13a)BC introduces support for virtual interface bundling on the Cisco uBR10012 universal broadband router and the Cisco uBR10-MC5X20S/U Broadband Processing Engine (BPE), and the Cisco uBR7246VXR router.

In prior Cisco IOS releases, cable interface bundling was limited to physical interfaces as master or slave interfaces, and **show** commands did not supply bundle information.

Virtual interface bundling removes the prior concepts of master and slave interfaces, and introduces these additional changes:

- Virtual interface bundling uses *bundle interface* and *bundle members* instead of master and slave interfaces.
- The virtual bundle interface is virtually defined, as with IP loopback addresses, for example.
- Virtual interface bundling supports bundle information in multiple **show ip interface** commands.

Virtual interface bundling prevents loss of connectivity on physical interfaces should there be a failure, problematic online insertion and removal (OIR) of one line card in the bundle, or erroneous removal of configuration on the master interface.

Virtual interface bundling supports and governs the following Layer 3 settings for the bundle member interfaces:

- IP address
- IP helper-address
- source-verify and lease-timer functions
- cable dhcp-giaddr (The giaddr field is set to the IP address of the DHCP client.)
- Protocol Independent Multicast (PIM)
- Access control lists (ACLs)
- Sub-interfaces

For additional configuration information, examples, and guidelines for virtual interface bundling, refer to the following documents on Cisco.com:

- *Cable Interface Bundling and Virtual Interface Bundling for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmmts/feature/guide/ufg\\_bund.html](http://www.cisco.com/en/US/docs/cable/cmmts/feature/guide/ufg_bund.html)
- *Virtual Interfaces and Frequency Stacking Configuration on MC5x20S and MC28U Line Cards*  
[http://www.cisco.com/en/US/tech/tk86/tk804/technologies\\_white\\_paper09186a0080232b49.shtml](http://www.cisco.com/en/US/tech/tk86/tk804/technologies_white_paper09186a0080232b49.shtml)
- *Virtual Interfaces on the Cisco uBR10-MC5X20S/U Card*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmmts\\_cbl\\_if\\_bundlg\\_ps2209\\_TS\\_D\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmmts_cbl_if_bundlg_ps2209_TS_D_Products_Configuration_Guide_Chapter.html)

## **New Hardware Features in Cisco IOS Release 12.3(9a)BC9**

There are no new hardware features supported in Cisco IOS Release 12.3(9a)BC9.

## **New Software Features in Cisco IOS Release 12.3(9a)BC9**

There are no new software features supported in Cisco IOS Release 12.3(9a)BC9.

## **New Hardware Features in Cisco IOS Release 12.3(9a)BC8**

There are no new hardware features supported in Cisco IOS Release 12.3(9a)BC8.

## **New Software Features in Cisco IOS Release 12.3(9a)BC8**

There are no new software features supported in Cisco IOS Release 12.3(9a)BC8.

## **New Hardware Features in Cisco IOS Release 12.3(9a)BC7**

There are no new hardware features supported in Cisco IOS Release 12.3(9a)BC7.

## **New Software Features in Cisco IOS Release 12.3(9a)BC7**

There are no new software features supported in Cisco IOS Release 12.3(9a)BC7.

## **New Hardware Features in Cisco IOS Release 12.3(9a)BC6**

There are no new hardware features supported in Cisco IOS Release 12.3(9a)BC6.

## **New Software Features in Cisco IOS Release 12.3(9a)BC6**

There are no new software features supported in Cisco IOS Release 12.3(9a)BC6.

## **New Hardware Features in Cisco IOS Release 12.3(9a)BC5**

There are no new hardware features supported in Cisco IOS Release 12.3(9a)BC5.

## **New Software Features in Cisco IOS Release 12.3(9a)BC5**

There are no new software features supported in Cisco IOS Release 12.3(9a)BC5.

## **New Hardware Features in Cisco IOS Release 12.3(9a)BC4**

There are no new hardware features supported in Cisco IOS Release 12.3(9a)BC4.

## **New Software Features in Cisco IOS Release 12.3(9a)BC4**

There are no new software features supported in Cisco IOS Release 12.3(9a)BC4.

## **New Hardware Features in Cisco IOS Release 12.3(9a)BC3**

There are no new hardware features supported in Cisco IOS Release 12.3(9a)BC3.

## **New Software Features in Cisco IOS Release 12.3(9a)BC3**

There are no new software features supported in Cisco IOS Release 12.3(9a)BC3.

## **New Hardware Features in Cisco IOS Release 12.3(9a)BC2**

There are no new hardware features supported in Cisco IOS Release 12.3(9a)BC2.

## **New Software Features in Cisco IOS Release 12.3(9a)BC2**

There are no new software features supported in Cisco IOS Release 12.3(9a)BC2.

## **New Hardware Features in Cisco IOS Release 12.3(9a)BC1**

There are no new hardware features supported in Cisco IOS Release 12.3(9a)BC1.

## **New Software Features in Cisco IOS Release 12.3(9a)BC1**

There are no new software features supported in Cisco IOS Release 12.3(9a)BC1.

## New Hardware Features in Cisco IOS Release 12.3(9a)BC

The following hardware features are new in Cisco IOS Release 12.3(9a)BC:

### Cisco uBR10-MC5X20S/U Broadband Processing Engine

Commencing with Cisco IOS Release 12.3(9a)BC, the Cisco uBR10-MC5X20S/U cable interface line card supports these additional DOCSIS and High Availability features on the Cisco uBR10012 CMTS:

- [PacketCable 1.0 With CALEA](#)
- [Virtual Interface and Frequency Stacking Support on the Cisco uBR10-MC5X20S/U BPE](#)
- [Virtual Interface Support for HCCP N+1 Redundancy](#)

### Cisco uBR10012 OC-48 DPT/POS Interface Module Support for the Cisco uBR10012 Performance Routing Engine 2 (PRE2) Modules

The Cisco uBR10012 OC-48 DPT/POS interface module supports both PRE1 and PRE2 performance routing engine modules in the Cisco uBR10012 router chassis. The Cisco OC-48 DPT/POS interface module is a dual-mode module, providing interface support for Packet over SONET (POS) or Spatial Reuse Protocol (SRP).

Cisco IOS Release 12.3(9a)BC introduces support for the Cisco uBR10012 OC-48 DPT/POS interface module with these additional DOCSIS and High Availability features on the Cisco uBR10012 CMTS:

- [NetFlow Accounting Versions 5 and 8 Support](#)
- [EtherChannel Support on the Cisco uBR10012 Universal Broadband Router](#)
- [Transparent LAN Service \(TLS\) on the Cisco uBR10012 Router with IEEE 802.1Q](#)

For additional information about installing and configuring the Cisco uBR10012 OC-48 DPT/POS interface module, refer to these documents on Cisco.com:

- *Cisco uBR10012 OC-48 DPT/POS Interface Module* (FRU Installation Guide)  
[http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/field\\_replaceable\\_units/ub\\_oc48.html](http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/installation/field_replaceable_units/ub_oc48.html)
- *Configuring the Cisco uBR10012 OC-48 DPT/POS Interface Module*  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/cable/line\\_cards/ubr\\_oc48\\_dpt\\_pos/configuration/guide/oc48pre2.html](http://www.cisco.com/en/US/docs/interfaces_modules/cable/line_cards/ubr_oc48_dpt_pos/configuration/guide/oc48pre2.html)

### Cisco uBR10012 Performance Routing Engine 2 (PRE2) Modules

Cisco IOS Release 12.3(9a)BC introduces support for the Cisco uBR10012 performance routing engine 2 (PRE2) route processing modules.

The Cisco uBR10012, which is qualified for PacketCable 1.0, Data over Cable Service Interface Specifications (DOCSIS) 1.1 and EuroDOCSIS 1.1, is built to meet the current and future needs of multiple system operators (MSOs). With full Layer 3 routing capabilities and industry-leading capacity and scalability, the Cisco uBR10012 delivers the highest level of performance for mass deployment of next-generation IP services.

The Cisco uBR10012 is designed to meet the services, performance, and reliability required for large-scale multiservice applications. The Cisco uBR10012 allows cable providers to deliver value-added IP services with consistent high performance. Based on Cisco IOS® Software—the standard in routing technology—the Cisco uBR10012 offers the most advanced networking and routing options available.

The Cisco uBR10012 features these components:

- Eight cable line cards to connect to the cable plant
- Four high-performance WAN interfaces to connect to the IP backbone and external networks
- Two Cisco Timing, Communication, and Control Plus (TCC+) cards to monitor the line cards and power supply
- Two Cisco Performance Routing Engine (PRE) modules with Parallel Express Forwarding (PXF) processors for consistent, high-performance throughput, even with multiple services enabled
- Two Power Entry Modules (PEMs) for uninterrupted power supply

Benefits of the Cisco uBR10012 PRE2 include the following:

- Provides up to 6.2 mpps of processing power in the Cisco uBR10012 router
- Backplane supports up to 6.4 Gbps duplex per slot
- Uses Cisco patented PXF technology to provide maximum IP services performance
- Supports processor redundancy—for enabling 99.999-percent network uptime
- Supports Route Processor Redundancy Plus (RPR+) High Availability functions in the Cisco uBR10012 CMTS headend

Table 5 provides additional details about the features and benefits of the Cisco uBR10012 PRE2.

**Table 5**      **Features and Benefits of Cisco uBR10012 PRE2**

Features	Benefits
Provides up to 6.2-mpps processing.	The Cisco uBR10012 router with PRE2 provides the IP services and performance that service providers require when deploying new revenue-generating services. In contrast to other CMTS products that support only distributed processing or only centralized processing, the Cisco uBR10012 supports a mix of distributed, centralized, and parallel processing. This ensures optimized performance to a comprehensive suite of line-rate IP services.
Uses Cisco patented PXF technology to provide maximum IP services performance.	PXF technology provides the Cisco uBR10012 router with performance and consistent high throughput, even with multiple, simultaneous services enabled. Using PXF, the Cisco uBR10012 router enables service providers to turn on multiple services without experiencing performance degradation. This is crucial when service providers look to upgrade customers to new types of services. In addition, PXF is a software-based technology that enables the Cisco uBR10012 router to implement new services without upgrading hardware—thereby providing investment protection and saving customers time and money.
Supports processor redundancy—for enabling 99.999-percent network uptime.	Each Cisco uBR10012 chassis supports up to two PRE2 modules for redundancy. The Cisco uBR10012 router is designed to support 99.999-percent uptime and coupled with a superior set of high-availability features and functions.

## Upgrading from Cisco uBR10012 PRE or PRE1 Modules to Cisco uBR10012 PRE2 Modules

For information about insertion, removal and upgrade of Field Replaceable Units such as the PRE2 modules, refer to the following document on Cisco.com:

- *Cisco uBR10012 Universal Broadband Router Performance Routing Engine Module 2*  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/cable/performance\\_routing\\_engine/installation/guide/pre5096.html](http://www.cisco.com/en/US/docs/interfaces_modules/cable/performance_routing_engine/installation/guide/pre5096.html)

## DOCSIS System Interoperability on the Cisco uBR10012 CMTS

This section describes the operation of primary interoperability features in the Cisco uBR10012 router. For additional DOCSIS information, refer to the following document on Cisco.com:

- *DOCSIS 1.1 for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_docs.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_docs.html)

### DOCSIS 1.0 Baseline Privacy

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

To enable BPI, choose software at both the CMTS and cable modem that support this mode of operation. Select a Cisco IOS image that supports BPI. BPI must be enabled using the DOCSIS configuration file.

The cable modem must also support BPI. Cable modems must have factory-installed RSA private/public key pairs to support internal algorithms to generate key pairs prior to first BPI establishment.




---

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

---

### Cable Modem Interoperability

- The Cisco uBR10012 router supports DOCSIS-based two-way interoperability for cable modems that support basic Internet access, Voice over IP (VoIP), or Virtual Private Networks (VPNs).
- EuroDOCSIS cable modems or set-top boxes (STBs) with integrated EuroDOCSIS CMs using Cisco uBR-MC16E cable interface line cards and Cisco IOS Release 12.2(4)BC1 or higher. EuroDOCSIS operation support includes 8-MHz Phase Alternating Line (PAL) or Systeme Electronique Couleur Avec Memoire (SECAM) channel plans.

### DOCSIS 1.0 and 1.0+ Extensions

Earlier releases of Cisco IOS software for the uBR10012 router provide support for the original DOCSIS 1.0 standard, featuring basic best-effort data traffic and Internet access over the coaxial cable network. The DOCSIS 1.0+ extensions provides Quality of Service (QoS) enhancements for real-time traffic, such as voice calls, in anticipation of full DOCSIS 1.1 support.

**Note**

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

## DOCSIS 1.1 Extensions

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

- Enhanced Quality of Service (QoS) gives priority for real-time traffic such as voice and video.
  - The DOCSIS 1.0 QoS model (a Service IDs (SID) associated with a QoS profile) has been replaced with a service flow model (SFID). This allows greater flexibility in assigning QoS parameters to different types of traffic and in responding to changing bandwidth conditions. See the [“SFID Support for Multicast and Cable Interface Bundling”](#) section on page 110.
  - Multiple service flows per cable modem supported in either direction due to packet classifiers.
  - Support for multiple service flows per cable modem allows a single cable modem to support a combination of data, voice, and video traffic.
  - Greater granularity is available in QoS per cable modem (in either direction), using unidirectional service flows.
  - Dynamic MAC messages are supported to create, modify, and tear down QoS service flows dynamically when requested by a DOCSIS 1.1 cable modem.
- Several QoS models are supported for the upstream.
  - Best effort-Data traffic is sent on a non-guaranteed best-effort basis.
  - Committed Information Rate (CIR) supports the guaranteed minimum bandwidth for data traffic.
  - Unsolicited Grants (UGS) support constant bit rate (CBR) traffic, such as voice, that is characterized by fixed size packets at fixed intervals.
  - Real Time Polling (rtPS) supports Real Time service flows, such as video, that produce unicast, variable size packets at fixed intervals.
  - Unsolicited Grants with Activity Detection (USG-AD) support the combination of UGS and RTPS, to accommodate real time traffic that might have periods of inactivity (such as voice using silence suppression). The service flow uses UGS fixed grants while active, but switches to RTPS polling during periods of inactivity to avoid wasting unused bandwidth.
- Enhanced time-slot scheduling mechanisms support guaranteed delay/jitter sensitive traffic on the shared multiple access upstream link.
- Payload header suppression (PHS) conserves link-layer bandwidth by suppressing unnecessary packet headers on both upstream and downstream traffic flows.
- Layer 2 fragmentation on the upstream prevents large data packets from affecting real-time traffic, such as voice and video. Large data packets are fragmented and then transmitted in the timeslots that are available between the timeslots used for the real-time traffic.
- Concatenation allows a cable modem to send multiple MAC frames in the same timeslot, as opposed to making an individual grant request for each frame. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.

- DOCSIS 1.1 cable modems can coexist with DOCSIS 1.0 and 1.0+ cable modems in the same network—the Cisco uBR10012 router provides the levels of service that are appropriate for each cable modem.

## DOCSIS 1.1 Quality of Service

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

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

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

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

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

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

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

## New Software Features for Cisco IOS Release 12.3(9a)BC

This section describes the following new software features and CLI command changes for Cisco IOS Release 12.3(9a)BC and the Cisco uBR10012 router:

- [Cable ARP Filter Enhancement, page 99](#)
- [Cisco Broadband Troubleshooter 3.2, page 100](#)
- [Cisco CMTS Static CPE Override, page 101](#)
- [Cisco IOS Release 12.3\(9a\)BC Command-Line Interface \(CLI\) Enhancements, page 101](#)
- [DOCSIS Set-Top Gateway Issue 1.0, page 101](#)
- [Dynamic Shared Secret \(DMIC\) with OUI Exclusion, page 102](#)
- [EtherChannel Support on the Cisco uBR10012 Universal Broadband Router, page 102](#)

- [MIBs Changes and Updates in Cisco IOS Release 12.3\(9a\)BC](#), page 103
- [NetFlow Accounting Versions 5 and 8 Support](#), page 106
- [PacketCable 1.0 With CALEA](#), page 109
- [SFID Support for Multicast and Cable Interface Bundling](#), page 110
- [CBT 3.2 Spectrum Management Support with the Cisco uBR10-MC5X20S/U BPE](#), page 111
- [Subscriber Traffic Management \(STM\) Version 1.1](#), page 111
- [Transparent LAN Service \(TLS\) on the Cisco uBR10012 Router with IEEE 802.1Q](#), page 112
- [Usage Based Billing \(SAMIS\)](#), page 112
- [Virtual Interface and Frequency Stacking Support on the Cisco uBR10-MC5X20S/U BPE](#), page 112
- [Virtual Interface Support for HCCP N+1 Redundancy](#), page 113

## Cable ARP Filter Enhancement

The **cable arp filter** command, introduced with Cisco IOS Release 12.2(15)BC2b, enables service providers to filter ARP request and reply packets. This prevents a large volume of such packets from interfering with the other traffic on the cable network.

Cisco IOS Release 12.3(9a)BC introduces enhanced command option syntax for the **cable arp filter** command, where *number* and *window-size* values are optional for **reply-accept** and **request-send** settings.

To control the number of Address Resolution Protocol (ARP) packets that are allowable for each Service ID (SID) on a cable interface, use the **cable arp** command in cable interface configuration mode. To stop the filtering of ARP broadcasts for CMs, use the **no** form of this command.

```
cable arp filter {reply-accept number window-size | request-send number window-size}
```

```
no cable arp filter {reply-accept | request-send}
```

```
default cable arp filter {reply-accept | request-send}
```

### Syntax Description

<b>reply-accept</b> <i>number</i> <i>window-size</i>	<p>Configures the cable interface to accept only the specified <i>number</i> of ARP reply packets every <i>window-size</i> seconds for each active Service ID (SID) on that interface. The cable interface drops ARP reply packets for a SID that would exceed this number.</p> <ul style="list-style-type: none"> <li><i>number</i> = (Optional) Number of ARP reply packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If <i>number</i> is 0, the cable interface drops all ARP reply packets. If not specified, this value uses default.</li> <li><i>window-size</i> = (Optional) Size of the window time period, in seconds, in which to monitor ARP replies. The valid range is 1 to 5 seconds, with a default of 2 seconds.</li> </ul>
<b>request-send</b> <i>number</i> <i>window-size</i>	<p>Configures the cable interface to send only the specified <i>number</i> of ARP request packets every <i>window-size</i> seconds for each active SID on that interface. The cable interface drops ARP requests for a SID that would exceed this number.</p> <ul style="list-style-type: none"> <li><i>number</i> = (Optional) Number of ARP request packets that is allowed for each SID within the window time period. The allowable range is 0 to 20 packets, with a default of 4 packets. If <i>number</i> is 0, the cable interface does not send any ARP request packets.</li> <li><i>window-size</i> = (Optional) Size of the window time period, in seconds, in which to monitor ARP requests. The valid range is 1 to 5 seconds, with a default of 2 seconds.</li> </ul>

Cisco IOS Release 12.3(9a)BC also removes a prior caveat with HCCP Protect interfaces. Previously, in the event of a revert-back HCCP N+1 switchover, manual removal of **cable arp filter reply** and **cable arp filter request** configurations may have been required afterward on Protect interfaces.

For more information about ARP Filtering, refer to the following document on Cisco.com:

- Cable ARP Filtering*

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

## Cisco Broadband Troubleshooter 3.2

Cisco IOS Release 12.3(9a)BC introduces support for the Cisco Broadband Troubleshooter (CBT) Version 3.2 on the Cisco uBR10012 universal broadband router, with newly supported interoperability for the following additional software features:

- [CBT 3.2 Spectrum Management Support with the Cisco uBR10-MC5X20S/U BPE, page 111](#)
- [Subscriber Traffic Management \(STM\) Version 1.1, page 111](#)

Multiple Service Operators (MSO) provide a variety of services such as TV, video on demand, data, and voice telephony to subscribers. Network Administrators and radio frequency (RF) technicians need specialized tools to resolve RF problems in the MSO's cable plant. Cisco Broadband Troubleshooter 3.2 (CBT 3.2) is a simple, easy-to-use tool designed to accurately recognize and resolve such issues.

The user can select up to three different cable modems (CMs) under the same CMTS or three different upstreams under the same CMTS. In addition, CBT 3.2 introduces the ability to display upstreams and cable modems combined (mixed) on the same trace window for monitoring and for playback.

**Note**

---

CBT 3.2 resolves the former CBT 3.1 caveat CSCee03388. With CBT 3.1, trace windows did not support the *mixing* of upstreams or cable modems.

---

For additional information about CBT 3.2, spectrum management and STM 1.1, refer to the following documents on Cisco.com:

- *Release Notes for Cisco Broadband Troubleshooter Release 3.2*  
[http://www.cisco.com/en/US/products/sw/netmgtsw/ps530/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps530/prod_release_notes_list.html)
- *Spectrum Management for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_spec.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_spec.html)
- *Subscriber Traffic Management for the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/ubsubmon.html>

## Cisco CMTS Static CPE Override

The **cable submgmt static-cpe-override** command enables Multiple Service Operators (MSOs) to override network DHCP settings on CPE devices when performing troubleshooting with a laptop computer and console connection to the Cisco universal broadband router.

For additional information about using the **cable submgmt static-cpe-override** command, refer to these documents on Cisco.com:

- “cable submgmt default” section on page 154
- *Cisco CMTS Static CPE Override*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/stat\\_cpe.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/stat_cpe.html)
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## Cisco IOS Release 12.3(9a)BC Command-Line Interface (CLI) Enhancements

Cisco IOS Release 12.3(9a)BC introduces or enhances the following CLI commands for the Cisco uBR10012 router:

- cable arp filter
- [cable logging layer2events](#)
- [cable source-verify](#)
- [show cable tech-support](#)
- [show controllers cable](#)
- [show tech-support](#)

For additional information about these command changes, refer to these resources:

- “Related Documentation” section on page 770
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## DOCSIS Set-Top Gateway Issue 1.0

Cisco IOS Release 12.3(9a)BC introduces support for DOCSIS Set-Top Gateway (DSG) Issue 1.0 on the Cisco uBR10012 universal broadband router. The DOCSIS Set-Top Gateway (DSG) feature allows the Cisco CMTS to provide a class of cable services known as out-of-band (OOB) messaging to set-top boxes (STBs) over existing DOCSIS networks. This allows MSOs and other service providers to combine both DOCSIS and STB operations over one, open, vendor-independent network, without any change to the existing network or cable modems.

DSG is a CableLabs® specification that allows the Cisco CMTS to provide a class of cable services known as out-of-band (OOB) messaging to set-top boxes (STBs) over existing Data-over-Cable Service Interface Specifications (DOCSIS) cable networks. DSG 1.0 allows cable Multi-System Operators (MSOs) and other service providers to combine both DOCSIS and STB operations over a single, open and vendor-independent network without requiring any changes to the existing DOCSIS network infrastructure.

At the time of this Cisco publication, the CableLabs® DOCSIS DSG specification is in the current status of “Issued” as characterized by stability, rigorous review in industry and cross-vendor interoperability.

For additional information about configuring and using DSG 1.0 on the Cisco uBR10012 router, refer to the following document on Cisco.com:

- *DOCSIS Set-Top Gateway for the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrdsdg12.html>

## Dynamic Shared Secret (DMIC) with OUI Exclusion

Cisco IOS Release 12.3(9a)BC introduces the option of *excluding* the Organizational Unique Identifiers (OUIs) from being subjected to the DMIC check. The new **cable dynamic-secret exclude** command allow specific cable modems to be excluded from the Dynamic Shared Secret feature on the following Cisco CMTS platforms:

- Cisco uBR7246VXR universal broadband router
- Cisco uBR10012 universal broadband router

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 additional command information, refer to the following document on Cisco.com:

- *Configuring a Dynamic Shared Secret for the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrdmic.html>
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## EtherChannel Support on the Cisco uBR10012 Universal Broadband Router

Cisco IOS Release 12.3(9a)BC introduces support for Gigabit EtherChannel (GEC) on the Cisco uBR10012 universal broadband router with the PRE2 performance routing engine modules. Cisco IOS Release 12.3(9) supports Gigabit Ethernet interfaces for IEEE 802.1Q inter-VLAN trunking with increased bandwidth on the Cisco uBR10012 router.



### Note

FastEtherChannel (FEC) interfaces and ATM trunking are not supported on the Cisco uBR10012 router.



### Note

Cisco IOS Release 12.3(9a)BC introduces support for Gigabit EtherChannel (GEC) on the Cisco uBR10012 universal broadband router with the PRE2 performance routing engine modules.

EtherChannel provides Gigabit Ethernet (GE) speeds by grouping multiple GE-speed ports into a logical port channel that supports speeds up to 8 Gbps. This provides fault-tolerant, high-speed links between switches, routers and servers.

Trunking is configured between the switch and the router to provide inter-VLAN communication over the network. Trunking carries traffic from several VLANs over a point-to-point link between the two network devices. In a campus network, trunking is configured over an EtherChannel link to carry the multiple VLAN information over a high-bandwidth channel.

For additional information about configuring EtherChannel on the Cisco uBR10012 router, refer to the following document on Cisco.com:

- *EtherChannel on the Cisco Cable Modem Termination System*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_ethr.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_ethr.html)

## MIBs Changes and Updates in Cisco IOS Release 12.3(9a)BC

Cisco IOS Release 12.3(9a)BC adds the following new MIB support for the Cisco uBR10012 router.

- [CISCO-CABLE-METERING-MIB](#)
- [CISCO-CABLE-QOS-MONITOR MIB](#)
- [CISCO-CABLE-SPECTRUM-MIB](#)
- [CISCO-ENHANCED-MEMPOOL-MIB](#)
- [CISCO-PROCESS-MIB](#)
- [DOCS-QOS-MIB](#)

For additional information about MIBs for the Cisco CMTS, refer to the following resources on Cisco.com:

- *Cisco CMTS Universal Broadband Router MIB Specifications Guide*  
<http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html>
- SNMP Object Navigator  
<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en>

## CISCO-CABLE-METERING-MIB

The CISCO-CABLE-METERING-MIB contains objects that provide subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format, also known as Usage-Based Billing on the Cisco CMTS. This format is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

The MODULE-IDENTITY for the CISCO-CABLE-METERING-MIB is `ciscoCableMeteringMIB`, and its top-level OID is 1.3.6.1.4.1.9.9.424 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCableMeteringMIB).



### Note

Refer to the *Cisco CMTS Universal Broadband Router MIB Specifications Guide* on Cisco.com for additional information and MIBs constraints.

## Additional Information

For additional SAMIS information, refer to the following resources:

- “Usage Based Billing (SAMIS)” section on page 112
- *Usage Based Billing for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_use-bsd\\_bill\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_use-bsd_bill_ps2209_TSD_Products_Configuration_Guide_Chapter.html)

## CISCO-CABLE-QOS-MONITOR MIB

Cisco IOS Release 12.3(9a)BC introduces additional features for the CISCO-CABLE-QOS-MONITOR MIB, including the following:

- Clarified the descriptions of a number of objects.
- Added a number of objects in the ccqmCmtsEnforceRuleTable to support DOCSIS 1.1 and DOCSIS 2.0 cable modems and to support peak and off-peak monitoring.
- Added the ccqmCmtsIfBwUtilTable to provide thresholds for downstream/upstream bandwidth utilization.
- Deprecated and removed ccqmCmtsEnfRuleByteCount.



### Note

Refer to the *Cisco CMTS Universal Broadband Router MIB Specifications Guide* on Cisco.com for additional information and MIBs constraints.

## CISCO-CABLE-SPECTRUM-MIB

Cisco IOS Release 12.3(9) introduces support for the CISCO-CABLE-SPECTRUM-MIB on the Cisco uBR10012 universal broadband router, with these additional MIB object enhancements:

- ccsFlapListMaxSize and ccsFlapListCurrentSize SNMP objects provide additional description for cable flap lists.
- Added the ccsCmFlapTable to replace the ccsFlapTable. The new object uses `downstream`, `upstream` and `Mac` as indices to replace the ccsFlapTable object.
- The enhanced ccsSNRRequestTable object provides a table of SNR requests with modified description.
- Added the ccsUpSpecMgmtUpperBoundFreq object to assist with spectrum management on the Cisco CMTS.
- Added the ccsCompliance5 object.
- Added ccsCmFlapResetNow to reset the flap list for a particular cable modem.
- Updated the descriptions for ccsFlapListMaxSize, ccsFlapListCurrentSize, and ccsSNRRequestTable.

The following objects are also now deprecated:

- ccsFlapPowerAdjustThreshold
- ccsFlapMissThreshold
- ccsFlapResetAll
- ccsFlapClearAll

- ccsFlapLastClearTime

The maximum number of entries in the flap-list was changed from a maximum of 8191 for the entire router, to the following:

- 8191 entries for each Broadband Processing Engine (BPE) cable interface, such as the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR10-MC5X20S/U.
- 8191 maximum flap-list entries for all non-BPE cable interfaces, such as the Cisco uBR-MC16C, Cisco uBR-MC16S, and Cisco uBR-MC28C.

Two objects are now used to track the flap list size:

- ccsFlapListMaxSize—Reflects the flap list size, as configured by the **cable flap-list size** command.
- ccsFlapListCurrentSize—Reflects the current size of the flap list for each MAC domain (downstream).

**Note**

Refer to the [Cisco CMTS Universal Broadband Router MIB Specifications Guide](#) on Cisco.com for additional information and MIBs constraints.

## CISCO-ENHANCED-MEMPOOL-MIB

Cisco IOS Release 12.3(9) introduces support for the CISCO-CABLE-SPECTRUM-MIB on the Cisco uBR10012 universal broadband router. The CISCO-ENHANCED-MEMPOOL-MIB enables you to monitor CPU and memory utilization for “intelligent” line cards and broadband processing engines on the Cisco uBR10012 router. These include the Cisco MC16X and MC28X series line cards.

**Note**

Refer to the [Cisco CMTS Universal Broadband Router MIB Specifications Guide](#) on Cisco.com for additional information and MIBs constraints.

## CISCO-PROCESS-MIB

Cisco IOS Release 12.3(9) introduces support for the CISCO-PROCESS-MIB on the Cisco uBR10012 universal broadband router with PRE2 modules. The CISCO-PROCESS-MIB enables you to monitor CPU and memory utilization for RF cards, cable interface line cards and broadband processing engines on the Cisco uBR10012 router.

**Note**

Refer to the [Cisco CMTS Universal Broadband Router MIB Specifications Guide](#) on Cisco.com for additional information and MIBs constraints.

## DOCS-QOS-MIB

Cisco IOS Release 12.3(9) introduces additional MIB object enhancements for the DOCS-QOS-MIB on the Cisco uBR10012 universal broadband router:

- Updated with the DOCSIS operations support system interface (OSSI) v2.0-N-04.0139-2.
- The default values of docsQosPktClassIpSourceMask and docsQosPktClassIpDestMask objects are set to 0xFFFFFFFF.



### Note

Refer to the [Cisco CMTS Universal Broadband Router MIB Specifications Guide](#) on Cisco.com for additional information and MIBs constraints.

## DSG-IF-MIB

The DSG-IF-MIB defines objects that are used to configure, control, and monitor the operation of the DOCSIS Set-top Gateway (DSG) 1.0 feature on Cisco uBR7200 series and Cisco uBR10012 routers.



### Note

The MODULE-IDENTITY for the DSG-IF-MIB is dsgIfMib, and its top-level OID is 1.3.6.1.4.1.9.9.999 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.dsgIfMib). Because this is an experimental MIB, its top-level OID is expected to change when the DSG specifications are finalized.



### Note

Refer to the [Cisco CMTS Universal Broadband Router MIB Specifications Guide](#) on Cisco.com for additional information and MIBs constraints.

## NetFlow Accounting Versions 5 and 8 Support

Cisco IOS Release 12.3(9a)BC introduces support for NetFlow Accounting Versions 5 and 8 on the Cisco uBR10012 router.



### Note

The Cisco uBR10012 router requires the PRE2 performance routing engine module to support NetFlow in Cisco IOS Release 12.3(9a)BC, and later releases in the 12.3 BC train. Also note that performance with packets-per-second (PPS) is reduced by 50% when NetFlow is enabled, as two passes per packet are required.

NetFlow enables you to collect traffic flow statistics on your routing devices. NetFlow provides network administrators with access to “call detail recording” information from their data networks. Exported NetFlow data can be used for a variety of purposes, including network management and planning, enterprise accounting and departmental chargebacks, ISP billing, data warehousing and data mining for marketing purposes.

NetFlow is based on identifying packet flows for ingress IP packets. It does not require any connection-setup protocol either between routers or to any other networking device or end station and does not require any change externally—either to the traffic or packets themselves or to any other networking device.

NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, NetFlow is performed independently on each internetworking device, it need not be operational on each router in the network. Using NetFlow Data

Export (NDE), you can export data to a remote workstation for data collection and further processing. Network planners can selectively invoke NDE on a router or on a per-subinterface basis to gain traffic performance, control, or accounting benefits in specific network locations.

## NetFlow Version 5 Features and Format

NetFlow exports flow information in UDP datagrams in one of two formats. The version 1 format was the initially released version, and version 5 is a later enhancement to add Border Gateway Protocol (BGP) autonomous system (AS) information and flow sequence numbers.

In NetFlow Version 1 and Version 5 formats, the datagram consists of a header and one or more flow records. The first field of the header contains the version number of the export datagram. Typically, a receiving application that accepts either format allocates a buffer big enough for the biggest possible datagram from either format and uses the version from the header to determine how to interpret the datagram. The second field in the header is the number of records in the datagram and should be used to index through the records.

All fields in either version 1 or version 5 formats are in network byte order. Table 5 and Table 6 describe the data format for version 1, and Table 7 and Table 8 describe the data format for version 5.

We recommend that receiving applications check datagrams to ensure that the datagrams are from a valid NetFlow source. We recommend you first check the size of the datagram to make sure it is at least long enough to contain the version and count fields. Next we recommend you verify that the version is valid (1 or 5) and that the number of received bytes is enough for the header and count flow records (using the appropriate version).

Because NetFlow export uses UDP to send export datagrams, it is possible for datagrams to be lost. To determine whether or not flow export information is lost, the version 5 header format contains a flow sequence number. The sequence number is equal to the sequence number of the previous plus the number of flows in the previous datagram. After receiving a new datagram, the receiving application can subtract the expected sequence number from the sequence number in the header to get the number of missed flows.

Table 6 lists the byte definitions for NetFlow Version 5 header format.

**Table 6** NetFlow Version 5 Header Format

Bytes	Content	Description
0-3	version and count	NetFlow export format version number and number of flows exported in this packet (1-30). <sup>1</sup>
4-7	SysUptime	Current time in milliseconds since router booted
8-11	unix_secs	Current seconds since 0000 UTC 1970.
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970.
16-19	flow_sequence	Sequence counter of total flows seen.
20-23	reserved	Unused (zero) bytes.

1. NetFlow Version 5 export packets (set with **ip flow-export** command) allow the number of records stored in the datagram to be a variable between 1 and 30.

Table 7 lists the byte definitions for Version 5 flow record format.

**Table 7 NetFlow Version 5 Flow Record Format**

Bytes	Content	Description
0-3	srcaddr	Source IP address.
4-7	dstaddr	Destination IP address.
8-11	nexthop	Next hop router's IP address.
12-15	input and output	Input and output interface's SNMP index.
16-19	dPkts	Packets in the flow.
20-23	dOctets	Total number of Layer 3 bytes in the flow's packets.
24-27	First	SysUptime at start of flow.
28-31	Last	SysUptime at the time the last packet of flow was received.
32-35	srcport and dstport	TCP/UDP source and destination port number or equivalent.
36-39	pad1, tcp_flags, prot, and tos	Unused (zero) byte, Cumulative OR of TCP flags, IP protocol (for example, 6=TCP, 17=UDP), and IP type-of-service.
40-43	src_as and dst_as	AS of the source and destination, either origin or peer.
44-47	src_mask, dst_mask, and pad2	Source and destination address prefix mask bits, pad 2 is unused (zero) bytes.

## NetFlow Version 8 Features and Format

NetFlow exports flow information in UDP datagrams in one of several formats. Version 8, a new data export version, has been added to support data exports from aggregation caches. Version 8 allows for export datagrams to contain a subset of the usual version 5 export data, which is valid for a particular aggregations scheme type.

Figure 1 illustrates the NetFlow Version 8 header format.

**Figure 1 Version 8 Header Format**

Version		Count	
System uptime			
UNIX seconds			
UNIX nanoseconds			
Sequence number			
Engine type	Engine ID	Aggregation	Aggregation version
Reserved			

26467

Table 8 lists definitions for terms used in the version 8 header.

**Table 8 Terms and Definitions for Version 8 Headers**

Term	Definition
Version	The flow export format version number. In this case, the number is “8”.
Count	The number of export records in the datagram.
System Uptime	The number of milliseconds since the router was last booted.
UNIX Seconds	The number of seconds since 0000 Universal Time Code (UTC) 1970.
UNIX Nanoseconds	The number of residual nanoseconds since 0000UTC 1970.
Sequence Number	Sequence counter of total flows sent for this export stream.
Engine Type	The type of switching engine. RP=0 and LC=1.
Engine ID	The slot number of the NetFlow switching engine.
Aggregation	The type of aggregation scheme being used.
Aggregation Version	The aggregation subformat version number. The current value is “2”.

## Additional Information about NetFlow on the Cisco CMTS

For additional information about configuring NetFlow Accounting on Cisco CMTS, refer to the following documents on Cisco.com:

- *NetFlow Overview, Version 5*  
[http://www.cisco.com/en/US/docs/net\\_mgmt/netflow\\_collection\\_engine/5.0/user/guide/overview.html](http://www.cisco.com/en/US/docs/net_mgmt/netflow_collection_engine/5.0/user/guide/overview.html)
- *NetFlow Overview, Version 8*  
[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod\\_presentation0900aecd80311f57.pdf](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_presentation0900aecd80311f57.pdf)
- *Configuring NetFlow (Versions 1 and 5)*  
[http://www.cisco.com/en/US/docs/net\\_mgmt/netflow\\_collection\\_engine/5.0/installation/guide/config.html](http://www.cisco.com/en/US/docs/net_mgmt/netflow_collection_engine/5.0/installation/guide/config.html)
- *Configuring NetFlow (Version 8)*  
[http://www.cisco.com/en/US/docs/net\\_mgmt/netflow\\_collection\\_engine/6.0/tier\\_one/installation/guide/install\\_1.html](http://www.cisco.com/en/US/docs/net_mgmt/netflow_collection_engine/6.0/tier_one/installation/guide/install_1.html) Toolkit
- Cisco IOS NetFlow White Papers  
[http://www.cisco.com/en/US/products/ps6601/prod\\_white\\_papers\\_list.html](http://www.cisco.com/en/US/products/ps6601/prod_white_papers_list.html)
- Cisco IOS Software Home Page for NetFlow  
[http://www.cisco.com/en/US/products/ps6601/products\\_ios\\_protocol\\_group\\_home.html](http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html)

## PacketCable 1.0 With CALEA

Cisco IOS Release 12.3(9a)BC introduces DOCSIS 1.1 support for PacketCable 1.0 with Communications Assistance for Law Enforcement Act (CALEA) on the Cisco uBR10012 universal broadband router with the Cisco uBR10-MC5X20S/U Broadband Processing Engine (BPE).

PacketCable is a program initiative from Cablelabs and its associated vendors to establish a standard way of providing packet-based, real-time video and other multimedia traffic over hybrid fiber-coaxial (HFC) cable networks. The PacketCable specification is built upon the Data-over-Cable System Interface Specifications (DOCSIS) 1.1, but it extends the DOCSIS protocol with several other protocols for use over non-cable networks, such as the Internet and the public switched telephone network (PSTN).

This allows PacketCable to be an end-to-end solution for traffic that originates or terminates on a cable network, simplifying the task of providing multimedia services over an infrastructure composed of disparate networks and media types. It also provides an integrated approach to end-to-end call signaling, provisioning, quality of service (QoS), security, billing, and network management.

Cisco IOS Release 12.2(11)BC1 and later releases in the Cisco IOS 12.3 release train support the PacketCable 1.0 specifications and the CALEA intercept capabilities of the PacketCable 1.1 specifications.

For additional information about configuring PacketCable on the Cisco CMTS, refer to the following document on Cisco.com:

- *Configuring PacketCable on the Cisco CMTS*

[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_pktcable\\_mm\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_pktcable_mm_ps2209_TSD_Products_Configuration_Guide_Chapter.html)

## SFID Support for Multicast and Cable Interface Bundling

Cisco IOS Release 12.3(9a)BC removes the prior restriction in Caveat CSCea45592 that prevented the creation of DOCSIS 1.1 upstream packet classifiers and service flow IDs (SFIDs) when configuring multicast groups with bundled cable interfaces. Cable interface bundling now supports SFIDs on Multicast groups.



**Note**

---

SFIDs map individual CPE devices to separate MPLS-Virtual Private Network (VPN) interfaces.

---



**Note**

---

Cisco IOS Release with the Cisco uBR10012 router does not support overlapping IP addresses with MPLS-VPN.

---

For additional configuration information, refer to the following document on Cisco.com:

- *Cable Interface Bundling for the Cisco CMTS*

[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_bund.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_bund.html)

## CBT 3.2 Spectrum Management Support with the Cisco uBR10-MC5X20S/U BPE

Cisco IOS Release 12.3(9a)BC introduces support for remote spectrum management for the Cisco uBR10012 router. Cisco uBR10012 spectrum management supports interoperability with these enhancements to the Cisco CMTS in Cisco IOS 12.3(9a)BC:

- [Cisco Broadband Troubleshooter 3.2, page 100](#), supporting the Cisco uBR10-MC5X20S/U Broadband Processing Engine (BPE)
- [Subscriber Traffic Management \(STM\) Version 1.1, page 111](#)

Additional supported spectrum management functions are available on the Cisco uBR10012 router. For a complete list, and the latest information about Spectrum Management on the Cisco uBR10012 router, refer to the following documents on Cisco.com:

- *Spectrum Management for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_spec.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_spec.html)
- *Release Notes for Cisco Broadband Troubleshooter Release 3.2*  
[http://www.cisco.com/en/US/products/sw/netmgts/ps530/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/netmgts/ps530/prod_release_notes_list.html)
- “Subscriber Traffic Management (STM) Version 1.1” section on page 111

## Subscriber Traffic Management (STM) Version 1.1

Cisco IOS Release 12.3(9a)BC introduces support for Subscriber Traffic Management (STM) through Version 1.1 on the Cisco uBR10012 universal broadband router. STM 1.1 supports DOCSIS 1.1-compliant cable modems.

The STM feature enables service providers to identify and control subscribers who exceed the maximum bandwidth allowed under their registered quality of service (QoS) profiles. STM is a simple bandwidth management tool which works as a low CPU alternative to Network-Based Application Recognition (NBAR) and access control lists (ACLs), however, using STM does not mean that NBAR and ACLs have to be turned off; STM can be applied along with NBAR and ACLs. STM 1.1 also works in conjunction with the Cisco Broadband Troubleshooter 3.2 to support additional network management and troubleshooting functions in the Cisco CMTS.

STM 1.1 extends earlier STM functions to monitor a subscriber's traffic on DOCSIS 1.1 primary service flows and supports these additional features:

- Cisco Broadband Troubleshooter (CBT) 3.2 supports STM 1.1.
- DOCSIS 1.0-compliant and DOCSIS 1.1-compliant cable modem are supported.
- Monitoring and application of traffic management policies are applied on a service-flow basis.
- Monitoring window duration increased from seven to 30 days.

For additional information about STM 1.1 and Cisco CBT 3.2, refer to the following document on Cisco.com:

- *Subscriber Traffic Management for the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/ubsubmon.html>
- *Release Notes for Cisco Broadband Troubleshooter Release 3.2*  
[http://www.cisco.com/en/US/products/sw/netmgts/ps530/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/netmgts/ps530/prod_release_notes_list.html)

## Transparent LAN Service (TLS) on the Cisco uBR10012 Router with IEEE 802.1Q

Cisco IOS 12.3(9a)BC introduces support for the Transparent LAN Service over Cable feature on the Cisco 10012 router. This feature enhances existing Wide Area Network (WAN) support to provide more flexible Managed Access for multiple Internet service provider (ISP) support over a hybrid fiber-coaxial (HFC) cable network.

This feature allows service providers to create a Layer 2 tunnel by mapping an upstream service identifier (SID) to an IEEE 802.1Q Virtual Local Area Network (VLAN).

For additional information about configuring TLS on the Cisco uBR10012 CMTS, refer to the following document on Cisco.com:

- *Transparent LAN Service over Cable*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/tls-cmts.html>



### Note

Cisco TLS for the Cisco uBR10012 router requires the PRE2 performance routing engine module with Cisco IOS Release 12.3(9a)BC or a later release in the Cisco IOS 12.3BC train.

## Usage Based Billing (SAMIS)

Cisco IOS Release 12.3(9a)BC introduces the Usage-Based Billing feature on the Cisco uBR10012 router. This feature provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. SAMIS is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

The [CISCO-CABLE-METERING-MIB](#) is also introduced with Cisco IOS Release 12.3(9a)BC in support of SAMIS.

For additional information about configuring and monitoring Usage-Based Billing (SAMIS) on the Cisco uBR10012 CMTS, refer to the following document on Cisco.com:

- *Usage Based Billing for the Cisco CMTS*  
<http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrsamis.html>

## Virtual Interface and Frequency Stacking Support on the Cisco uBR10-MC5X20S/U BPE

Virtual interfaces (VI) and frequency stacking (FS) are two features that allow user-configurable MAC domains and multiple frequencies on one physical connector.

- Virtual interfaces allow up to eight upstreams (USs) per downstream (DS). A virtual interface links an upstream (US) port to a physical connector.

Cisco IOS Release 12.3(9a)BC introduces [Virtual Interface Support for HCCP N+1 Redundancy](#) with the Cisco uBR10-MC5X20S/U BPE.

- Frequency stacking allows two frequencies to be configured on one physical connector.

Cisco IOS Release 12.3(9a)BC introduces support for frequency stacking on the Cisco uBR10012 router.

The Cisco uBR10-MC5X20S/UBPE can be configured (initially) to match the DS and US configuration of an existing line card, and then the cable operator can modify the configurations according to their needs. This supports different DS-to-US port ratios as such combination ratios evolve (1x6 » 1x4 » 1x1). For example, the line card can be used in 1x1 configuration for a business customer and in 1x7 configuration for residential customers.

For additional information about configuring virtual interfaces and frequency stacking, refer to the following document on Cisco.com:

- *Virtual Interfaces and Frequency Stacking Configuration on MC5x20S and MC28U Linecards*  
[http://www.cisco.com/en/US/tech/tk86/tk804/technologies\\_white\\_paper09186a0080232b49.shtml](http://www.cisco.com/en/US/tech/tk86/tk804/technologies_white_paper09186a0080232b49.shtml)
- *Configuring Virtual Interfaces on the Cisco uBR10-MC5X20S/U Card*  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/cable/broadband\\_processing\\_engines/ubr10\\_mc5x20s\\_u\\_h/feature/guide/mc5x2vif.html](http://www.cisco.com/en/US/docs/interfaces_modules/cable/broadband_processing_engines/ubr10_mc5x20s_u_h/feature/guide/mc5x2vif.html)

## Virtual Interface Support for HCCP N+1 Redundancy

Cisco IOS Release 12.3(9a)BC introduces support for HCCP N+1 Redundancy for virtual interfaces configured on the Cisco uBR10012 universal broadband router using the Cisco uBR10-MC5X20S/U BPE.

HCCP N+1 Redundancy is an important step toward high availability on CMTS and telecommunications networks that use broadband media. HCCP N+1 Redundancy can help limit Customer Premises Equipment (CPE) downtime by enabling robust automatic switchover and recovery in the event that there is a localized disruption in service.

Beginning with Cisco IOS Release 12.2(15)BC2a, HCCP N+1 Redundancy adds synchronization between HCCP Working interface configurations and those inherited upon switchover to HCCP Protect interfaces. This makes the configuration of both easier and switchover times faster.

For additional information about configuring virtual interfaces in HCCP N+1 redundancy on the Cisco CMTS, refer to the following document on Cisco.com:

- *N+1 Redundancy for the Cisco Cable Modem Termination System*  
[http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts\\_nplus1\\_redun\\_ps2209\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_nplus1_redun_ps2209_TSD_Products_Configuration_Guide_Chapter.html)
- *Configuring Virtual Interfaces on the Cisco uBR10-MC5X20S/U Card*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_bund.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_bund.html)

## MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, 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](mailto: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://tools.cisco.com/RPF/register/register.do>

## MIB Changes and Enhancements for Cisco IOS Release 12.3(21)BC:

The DOC-QOS-MIB enhancement in Cisco IOS Release 12.3(21)BC added new tables to support SNMP QoS MIB query time in a large scale system with much less CPU consumption. The overall performance is better in multiple SNMP query sessions on the six tables than a single session. However, this solution has the following restrictions:

- The ideal number of multiple sessions is around 7-10. Even though up to 128 multiple sessions are supported, it is not recommended to have more than 30 multiple sessions.
- The improvement may not be visible in a small scale system. For example less than 100 CM per LC.
- If multiple SNMP sessions all query the 6 enhanced DOCS-QOS-MIB tables with the same number of objects per session as the single-session query then the per session response time could be better than the single SNMP session with the same number of MIB objects. Please note, the aggregated CPU utilization for multiple sessions is still higher than the single session query on the CMTS. It is under the condition that both RP and line card CPU utilizations are not stressed.



Note

The number of multiple sessions should equal the number of parallel object queries.

## MIB Constraints and Notes

This MIB is supported only in Cisco IOS Release 12.2(4)BC1 through Release 12.2(11)BC3 to support DOCSIS 1.1 operations. The MIB is deprecated in later releases to conform with the DOCSIS 2.0 specifications.

**Table 9** *DOCS-QOS-MIB Constraints*

MIB Object	Notes
<code>docsQosCmtsMacToSrvFlowTable</code>	<p>Do not use GET-NEXT requests to retrieve the rows of this table, because it could require lengthy, time-consuming searches on the MAC address, which could consume excessive amounts of CPU processor time when the table is large. Instead, retrieve the individual rows using a GET request that uses the device's MAC address as the table index. This avoids possible performance problems and also ensures that the retrieved rows contain the most current, real-time data for those devices.</p> <p>A GET request for <code>docsQosCmtsMacToSrvFlowTable</code> returns NULL if the router is already processing another request for this table (either by an SNMP GET or CLI <b>show</b> command). A null is also returned if the router is processing a request for any other table that is indexed by CM or CPE MAC address, such as <code>cdxCmCpeEntry</code>, <code>cdrqCmtsCmStatusTable</code>, and <code>docsIfCmtsMacToCmTable</code>.</p> <p>Wait until the first request is done and then repeat the request for <code>docsQosCmtsMacToSrvFlowTable</code>.</p>
<code>docsQosParamSetTable</code>	<p>This table describes the set of DOCSIS 1.1 QOS parameters defined in a managed device.</p>

Table 9 DOCS-QOS-MIB Constraints (continued)

MIB Object	Notes
<ul style="list-style-type: none"> <li>docsQosParamSetMaxTrafficBurst</li> <li>docsQosServiceClassDirection</li> <li>docsQosServiceClassSchedulingType</li> <li>docsQosParamSetEntry**</li> </ul>	<p>Valid only for Best Effort, non-Real-Time Polling, and Real-Time Polling bursts. For all other bursts, this object reports 0.</p> <p>These objects must be set together as part of the same SET request when configuring a downstream service class.</p> <p>Identifies a unique set of QoS parameters.</p>
<b>docsQosServiceFlowStatsTable</b>	Reports the downstream traffic counters for cable modems that are provisioned for DOCSIS 1.1 and DOCSIS 2.0 operation. For DOCSIS 1.0 cable modems, use the cdxCmtsServiceExtTable in CISCO-DOCS-EXT-MIB.
<ul style="list-style-type: none"> <li>docsQosServiceFlowStatsEntry**</li> </ul>	Describes a set of service flow statistics. An entry in the table exists for each Service Flow ID. The ifIndex is an ifType of docsCableMaclayer(127)."
<b>docsQosPHSTable</b>	This table describes set of payload header suppression entries.
<ul style="list-style-type: none"> <li>docsQosPHSEntry**</li> </ul>	
<b>docsQosPktClassTable</b>	
<ul style="list-style-type: none"> <li>docsQosPktClassEntry**</li> </ul>	An entry in this table that provides a single packet classifier rule.
<b>docsQosServiceFlowTable</b>	
<ul style="list-style-type: none"> <li>docsQosServiceFlowEntry**</li> </ul>	Describes a service flow. An entry in the table exists for each Service Flow ID. The ifIndex is an ifType of docsCableMaclayer(127).
<b>docsQosUpstreamStatsTable</b>	
<ul style="list-style-type: none"> <li>docsQosUpstreamStatsEntry**</li> </ul>	Describes a set of upstream service flow statistics.
<b>docsQosServiceFlowLogTable</b>	Logs deleted DOCSIS 1.1 and DOCSIS 2.0 service flows, but this table does not contain any information until after logging is specifically enabled using the <b>cable sflog</b> command in global configuration mode.
<b>docsQosDynamicServiceStatsTable</b>	(not applicable for Docsis 1.0 modems)
<ul style="list-style-type: none"> <li>docsQosDCCReqs</li> <li>docsQosDCCRsp</li> <li>docsQosDCCAcks</li> <li>docsQosDCCs</li> </ul>	<p>Read-only. The number of Dynamic Channel Change Request messages traversing an interface. This count is nonzero only on downstream direction rows.</p> <p>Read-only. The number of Dynamic Channel Change Response messages traversing an interface. This count is nonzero only on upstream direction rows.</p> <p>Read-only. The number of Dynamic Channel Change Acknowledgement messages traversing an interface. This count is nonzero only on downstream direction rows.</p> <p>Read-only. The number of successful Dynamic Channel Change transactions. This count is nonzero only on downstream direction rows.</p>

**Table 9**      **DOCS-QOS-MIB Constraints (continued)**

<b>MIB Object</b>	<b>Notes</b>
<ul style="list-style-type: none"> <li>docsQosDCCFails</li> </ul>	Read-only. The number of failed Dynamic Channel Change transactions. This count is nonzero only on downstream direction rows.

---

\*\*The SNMP query sessions have been improved in these tables.

---

**Note**

For detailed information about load balancing and dynamic channel change on CMTS, go to the following URL:

[http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting\\_batch9/cmts1bg.html](http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting_batch9/cmts1bg.html)

---

## MIB Changes and Enhancements for Cisco IOS Release 12.3(17a)BC:

MIB enhancements in Cisco IOS Release 12.3(17a)BC provide enhanced management features that enable the Cisco uBR 7200 Series router and the Cisco uBR 10012 router to be managed through the Simple Network Management Protocol (SNMP). These enhanced management features allow you to:

- Use SNMP set and get requests to access information in Cisco CMTS universal broadband routers
- Reduce the amount of time and system resources required to perform functions like inventory management
- A standards-based technology (SNMP) for monitoring faults and performance on the router
- Support for SNMP versions (SNMPv1, SNMPv2c, and SNMPv3)
- Notification of faults, alarms, and conditions that can affect services

For a complete list of changes to the Cisco CMTS Universal Broadband Router MIB Specifications Guide, go to the Revision History table:

<http://www.cisco.com/en/US/docs/cable/cmts/mib/reference/guide/mibv5ubr.html>

## Important Notes

The following sections contain important notes about Cisco IOS Release 12.3(23)BC7 that apply to the Cisco uBR10012 universal broadband router universal broadband router.

## How to Upgrade to Cisco IOS Release 12.3(21)BC

In circumstances in which non-volatile memory (NVRAM) becomes corrupted on the Cisco CMTS, configurations and feature behavior may become corrupted or lost, looping behavior in NVRAM may result, and additional measures to resolve corrupted NVRAM and lost configurations would be required.

This issue can be generated by upgrading to later Cisco IOS releases from prior Cisco IOS releases that do not contain resolution to a specific and known issue. This issue is not limited to Cisco IOS releases installed on the Cisco universal broadband routers.

## Symptoms of Corrupted NVRAM

This issue is displayed with the following symptoms in the case of the Cisco CMTS:

- A router may display the following error message:
  - NV: Invalid Pointer value(6357F3CC) in private configuration structure

This error message is displayed either when the router boots, or when you enter one of the following commands:

- **write memory**
- **copy running-config startup-config**
- **copy file**
- **nvram:startup-config**

## Conditions of Corrupted NVRAM

This symptom is observed under the following conditions:

- The Cisco router runs one of the following Cisco IOS Releases, as the outgoing image to be upgraded:
  - Interim Cisco IOS Release 12.3(19.7)
  - Interim Cisco IOS Release 12.4(6.5)
  - Interim Cisco IOS Release 12.4(6.5)T
  - Certain later releases

When upgrading to Cisco IOS Release 12.3(21)BC, the following upgrade procedure prevents corruption to NVRAM, retains configurations made in earlier releases, and successfully installs Cisco IOS Release 12.3(21)BC images. This procedure is subject to the feature restrictions and prerequisites of Cisco IOS Release 12.3(21)BC, described in these release notes.

### Prerequisites

Cisco strongly recommends that you back up your configuration files prior to performing this upgrade, or any upgrade.

### SUMMARY STEPS

Perform these steps to upgrade to Cisco IOS 12.3(21)BC, after TFTP file transfer operations are complete.

1. **enable**
2. **configure terminal**
3. **erase /all nvram:**
4. **write memory**
5. **copy file**
6. **reload**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>erase /all nvram:</b> or</p> <p><b>erase nvram:</b> or</p> <p><b>write erase</b></p> <p><b>Example:</b> Router# erase /all nvram:</p>	<p>The first command option for this step erases the entire NVRAM.</p> <p>Either of the final two command options erase only the configuration files in NVRAM.</p>
Step 4	<p><b>write memory</b></p> <p><b>Example:</b> Router# write memory</p>	<p>(Optional) Copies the running configuration to startup configuration.</p>
Step 5	<p><b>copy file</b></p> <p><b>Example:</b> Router# copy &lt;saved-config&gt; startup-config</p>	<p>(Optional) Copies a saved configuration, if different from the running configuration, to the startup configuration.</p> <ul style="list-style-type: none"> <li><i>file</i>—saved configuration file to be copied to the startup configuration</li> </ul>
Step 6	<p><b>reload</b></p> <p><b>Example:</b> Router# reload</p>	<p>Boots the router with the latest Cisco IOS release image.</p>

## New Command Information for Cisco IOS Release 12.3(21)BC

Cisco IOS Release 12.3(21)BC introduces support and modifications to the following commands for Cisco Cable Modem Termination System (CMTS) universal broadband routers.

Refer to the following sections for more information:

- [cable throttle-ranging](#)
- [card](#)
- [clear cable modem reset](#)
- [hw-module reload](#)
- [hw-module shutdown](#)
- [show cable modem summary](#)

- [show cable modem wideband](#)
- [show interface wideband-cable](#)

## cable throttle-ranging

To enable faster cable modem registration times, use the **cable throttle-ranging** command in global configuration mode. To disable faster cable modem registration times, use the **no** form of this command.

**cable throttle-ranging**

**no cable throttle-ranging**

---

**Syntax Description** This command has no arguments or keywords

---

**Defaults** This command is disabled by default.

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.3(21)BC	This command was introduced.

---



---

**Usage Guidelines** The **cable throttle-ranging** command enables faster cable modem registration times on the CMTS. Reload the Cisco CMTS with a Cisco IOS Release 12.3(21)BC image and configure the **cable throttle-ranging** command on the CMTS. Once the **cable throttle-ranging** has been configured, save the new configuration and reload the Cisco CMTS again. Faster cable modem registration times will now be enabled on the Cisco CMTS.




---

**Note** The **cable throttle-ranging** command is only available on anubr10k CMTS.

---



---

**Examples** The following example shows how to enable Fast CM registration feature on a Cisco CMTS:

```
Router# cable throttle-ranging
Router(config)#
```

---

**Related Commands** There are no related commands for this command.

## card

To preprovision a slot in the Cisco uBR10012 universal broadband router for a particular interface card, so that you can configure the interface without it being physically present in the slot, use the **card** command in global configuration mode. To remove the preprovisioning for a card, so that the physical slot reports being empty, use the **no** form of this command.

```
card {slot/subslot | slot/subslot/bay} card-type
```

```
no card {slot/subslot | slot/subslot/bay}
```

### Syntax Description

slot/subslot	Identifies the chassis slot and subslot for the card. The following are the valid values: <ul style="list-style-type: none"> <li>slot = 1 to 8</li> <li>subslot = 0 or 1</li> </ul>
slot/subslot/bay	Identifies the chassis slot and subslot for the Cisco Wideband SIP, and the bay number in the SIP where the Cisco Wideband SPA is located. The following are the valid values: <ul style="list-style-type: none"> <li>slot = 1 to 3</li> <li>subslot = 0 or 1 (0 is always specified)</li> <li>bay = 0 (upper bay) or 1 (lower bay)</li> </ul>
card-type	Specifies the type of card that should be used to preprovision the slot. See <a href="#">Table 10</a> for a list of the supported cards.



### Note

The list of supported card types depends on the Cisco IOS software release being used. See the release notes for your release for the complete list of cards that are supported.

### Defaults

An empty card slot is not preprovisioned and cannot be configured or displayed.

### Command Modes

Global configuration

### Command History

Release	Modification
12.2(1)XF1	This command was introduced for the Cisco uBR10012 router, and for the following line cards: <ul style="list-style-type: none"> <li>Cisco uBR-LCP-MC28C cable interface line card</li> <li>Cisco uBR-LCP-MC28C-BNC cable interface line card</li> <li>Cisco uBR10-1GE Gigabit Ethernet (GigE) uplink line card</li> <li>Cisco uBR10-1OC12/P-SMI OC-12 POS uplink line card</li> </ul>
12.2(4)XF1	Support was added for the Cisco uBR-LCP-MC16C and Cisco uBR-LCP-MC16E cable interface line cards.

Release	Modification
12.2(4)BC1	Support was added for the Cisco uBR10-SRP-OC12SML DPT WAN uplink line card.
12.2(8)BC1	Support was added for the Cisco LCP2 line card processor, and all of its combinations with the supported cable interface line cards.
12.2(11)BC3	Support was added for the Cisco uBR10012 OC-48 DPT/POS Interface Module uplink line card and Cisco uBR-MC5X20S cable interface line card.
12.2(15)CX1	Support was added for the Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cable interface line cards.
12.2(15)BC2	Support was added for the Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, and Cisco uBR-MC5X20U cable interface line cards.
12.3(21)BC	Support was added for the Cisco Wideband SIP and Wideband SPA.

### Usage Guidelines

This command preprovisions a slot in the Cisco uBR10012 router to accept a particular line card, so that you can configure the interface without the card being physically present in the chassis. This command allows system administrators to plan for future configurations, without having to wait for the physical hardware to first arrive. When the line card does arrive, the installer can bring the card online by inserting the card into the chassis and connecting the necessary cables, without having to do any further configuration using the command-line interface.

The type of card must be appropriate for the slot being specified. Slots 1/1 and 2/1 are reserved for TCC+ utility cards. Slots 1/0 through 4/0 are reserved for network uplink line cards. Slot 5/0 through 8/1 are reserved for cable interface line cards. Slot 0/0 is reserved for the FastEthernet interface on the PRE1 module and cannot be specified in this command.

Table 10 lists the types of cards that are supported as *card-types* for the **card** command:

**Table 10** Card Types Supported by the **card** Command

Card Type	Description
<b>1cable-mc16c</b>	Preprovisions a slot for a Cisco uBR-LCP-MC16C or Cisco uBR-LCP2-MC16C cable interface line card.
<b>1cable-mc16e</b>	Preprovisions a slot for a Cisco uBR-LCP-MC16E or Cisco uBR-LCP2-MC16E cable interface line card.
<b>1cable-mc16s</b>	Preprovisions a slot for a Cisco uBR-LCP-MC16S or Cisco uBR-LCP2-MC16S cable interface line card.
<b>1gigethernet-1</b>	Preprovisions a slot for a Cisco uBR10-1GE Gigabit Ethernet (GigE) uplink line card.
<b>1oc12pos-1</b>	Preprovisions a slot for a Cisco uBR10-1OC12/P-SMI OC-12 POS uplink line card.
1oc48dpt-pos-1	Preprovisions a slot for a Cisco uBR10012 OC-48 DPT/POS Interface Module uplink line card.
24rfchannel-spa-1	Preprovisions a bay in the Cisco Wideband SIP for the Cisco 1-Gbps Wideband Shared Port Adapter (SPA).
<b>2cable-mc28bnc</b>	Preprovisions a slot for a Cisco uBR-LCP-MC28C-BNC or Cisco uBR-LCP2-MC28C-BNC cable interface line card.

**Table 10** Card Types Supported by the card Command (continued)

Card Type	Description
2cable-mc28c	Preprovisions a slot for a Cisco uBR-LCP-MC28C or Cisco uBR-LCP2-MC28C cable interface line card.
2cable-tccplus	Preprovisions a slot for a Timing, Control, and Communications Plus (TCC+) utility card. <b>Note</b> This option is informational only, because slots 1/1 and 2/1 can be used only for the TCC+ card.
2jacket-1	Preprovisions a slot for the Cisco Wideband SPA Interface Processor (SIP).
2oc12srp-sm-lr	Preprovisions a slot for a Cisco uBR10-SRP-OC12SML DPT WAN uplink line card.
5cable-mc520s-d	Preprovisions a slot for a Cisco uBR10-MC5X20S-D cable interface line card.
5cable-mc520u-d	Preprovisions a slot for a Cisco uBR10-MC5X20U-D cable interface line card.



**Tip**

When a card has been preprovisioned and is not physically present in the chassis, the **show interface** command for that slot displays the message “Hardware is not present.” Some **show** commands might also list the preprovisioned card in their displays. In addition, using the **card** command does not change the output of the ENTITY-MIB, which shows only the equipment that is physically installed in the router.

When a line card is inserted in the Cisco uBR10012 chassis, the router performs the following actions, depending on whether the card slot is preprovisioned for the card:

- If the inserted line card matches the type of line card preprovisioned for the slot, the system applies the preprovisioned configuration to the line card.
- If the line card slot was not preprovisioned, the system applies a basic configuration to the line card and adds that configuration to the running configuration file.
- If the line card slot was preprovisioned for one type of line card, but another type of line card has been inserted, the system replaces the preprovisioned configuration (in the running configuration file) with a basic configuration for the line card that was actually inserted. The startup configuration file is not changed.



**Tip**

Use the **show running-config | include card** command to display which slots, if any, are preprovisioned for a particular card type.

The **no card version of the** command removes the preprovisioning information from the given card slot. This also removes all configuration information for that card slot, as well as any information in the SNMP MIB database about the card and its card slot.

**Examples**

The following example shows a list of supported card types for Cisco IOS Release 12.2(8)BC1, and then shows that slot 8/0 is being preprovisioned for a Cisco uBR-LCP2-MC28C cable interface line card. The cable interface for slot 8/0 can then be configured.

```
Router# config t
Router(config)# card 5/0 ?
    1cable-mc16c    create a uBR10000 line card with MC16C
```

```

1cable-mc16e      create a uBR10000 line card with MC16E
1gigethernet-1   create a GE_1_PORT cardtype
1oc12pos-1       create a OC12POS_1_PORT cardtype
2cable-mc28bnc   create a uBR10000 line card with MC28C, BNC connector
2cable-mc28c     create a uBR10000 line card with MC28C
2oc12srp-sm-lr   create a uBR10000 oc12 SRP card with SM LR
Router(config)# card 8/0 2cable-mc28c
Router(config)# int c8/0
Router(config-if)#

```

The following example shows the output from the **show interface** command for a preprovisioned cable interface. The second line of the output shows that the hardware is not present.

```

Router# show interface c8/0/0
Cable8/0/0 is initializing, line protocol is down
  Hardware is not present
  Hardware is UBR10000 CLC, address is 0001.6440.d160 (bia 0001.6440.d160)
  MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation MCNS, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
Router#

```

The following examples show the two steps required to preprovision the Wideband SIP and Wideband SPA.

The Wideband SIP is preprovisioned with the **card** command and **2jacket-1** as the card type. For example:

```

Router# configure terminal
Router(config)# card 1/0 2jacket-1
Router(config)#

```

The Wideband SPA is preprovisioned with the **card** command and **24rfchannel-spa-1** as the card type. For example:

```

Router# configure terminal
Router(config)# card 1/0/0 24rfchannel-spa-1
Router(config)#

```

The preceding **card** command creates 12 wideband channels on the Wideband SPA.

## Related Commands

Command	Description
show interface cable	Displays the current configuration and status of a cable interface.

## clear cable modem reset

To remove one or more CMs from the Station Maintenance List and reset them, use the **clear cable modem reset** command in privileged EXEC mode.

```
clear cable modem {mac-addr | ip-addr | [cable slot/port] {all | oui string | reject} } reset
```

```
clear cable modem {mac-addr | ip-addr | [cable slot/subslot/port] {all | oui string | reject | wideband registered-traditional-docsis} } reset
```

### Syntax Description

mac-addr	Specifies the 48-bit hardware address (MAC address) of an individual CM, or of any CPE devices or hosts behind that CM.
ip-addr	Specifies the IP address of an individual CM, or of any CPE devices or hosts behind that CM.
cable slot/port	(Optional) Identifies the a interface and downstream port on the Cisco uBR7100 series and Cisco uBR7200 series routers.  On the Cisco uBR7100 series router, the only valid value is <b>1/0</b> . On the Cisco uBR7200 series router, <i>slot</i> can range from 3 to 6, and <i>port</i> can be 0 or 1, depending on the cable interface.
cable slot/subslot/port	(Optional) Identifies a cable interface on the Cisco uBR10012 router. The following are the valid values: <ul style="list-style-type: none"> <li>• <i>slot</i> = 5 to 8</li> <li>• <i>subslot</i> = 0 or 1</li> <li>• <i>port</i> = 0 to 4 (depending on the cable interface)</li> </ul>
all	Removes all the CMs from the Station Maintenance List. (This option is valid only on the Release 12.1 EC train.)
oui string	Removes and resets all CMs that match the specified Organization Unique Identifier (OUI). The <i>string</i> parameter can be either the three byte hexadecimal string (such as 00.00.0C) or a vendor name that has been defined using the <b>cable modem vendor</b> command.
reject	Removes and resets all CMs that are currently in one of the reject states (see the description of these states in the <b>show cable modem</b> command).
wideband registered-traditional-docsis	If you specify <b>wideband</b> , removes and resets all wideband CMs. If you specify <b>wideband registered-traditional-docsis</b> , removes and resets all wideband CMs that are registered as traditional DOCSIS modems.

### Defaults

No default behavior or values

### Command Modes

Privileged EXEC

**Command History**

Release	Modification
12.1(2) EC	This command was introduced.
12.2(4)BC1	Support was added to the Release 12.2 BC train.
12.2(11)BC2	Support was added for the <b>oui</b> and <b>reject</b> options.
12.2(11)BC3	The <b>all</b> option was removed from the Release 12.2 BC train, and replaced with the <i>interface</i> option.
12.2(15)BC1	The cable interface was made an optional keyword for this command.
12.3(21)BC	Support was added for the <b>wideband</b> and <b>registered-traditional-docsis</b> keywords.

**Usage Guidelines**

This command instructs the Cisco CMTS to stop sending DOCSIS station maintenance messages to one or more CMs, which effectively terminates the link to those CMs. A CM responds to this by resetting itself. Depending on when the CM received the last station maintenance message, it can take up to 30 seconds before the CM detects the missing station maintenance messages and resets itself.

In some circumstances, the customer premises equipment (CPE) devices behind a CM stops receiving traffic after the CM is reset. This is because the CMTS still has the CPE device listed in its address tables, but the CM does not after being reset, so the traffic passes through the CMTS but is dropped by the CM. To resolve this situation, the CPE device should simply send some type of traffic to the CM, such as a ping packet. (You can also resolve this situation by using the **clear arp-cache** command on the Cisco CMTS router to clear the router's address table, but this is not recommended, because it temporarily interrupts all traffic on the router.)

**Note**

The **clear cable modem all reset** command can result in the CPU utilization temporarily reaching 100 percent for a couple of minutes, as the CPU processes the command for all CMs. The CPU utilization will return to normal within a couple of minutes.

**Caution**

The **clear cable modem all reset** command should normally be used only on a test or lab network. If used on a large network, it could impact service for a significant period of time, as it would force all CMs to simultaneously reset and reregister with the Cisco CMTS.

**Tip**

You can also specify the MAC address or IP address for a CPE device or host, and the Cisco CMTS resets the CM that is associated with that CPE device in its internal database.

**Examples**

The following example shows how to reset the CM at 172.23.45.67:

```
Router# clear cable modem 172.23.45.67 reset
Router#
```

The following example shows how to reset all CMs that have a OUI that has been defined as having the vendor name of Cisco using the **cable modem vendor** command:

```
Router# clear cable modem oui Cisco reset
Router#
```

The following example shows how to reset all CMs that are currently in one of the reject states:

```
Router# clear cable modem reject reset
Router#
```

The following example shows how to reset all wideband CMs that are registered as traditional DOCSIS modems.:

```
Router# clear cable modem wideband registered-traditional-docsis reset
MAC Address      IP Address      I/F      MAC          Prim  BG  DSID  MD-DS-SG
                  State          Sid   ID
0018.6852.825c  80.18.0.9      C5/0/0/U0  online      1     0   256   N/A
0018.6852.8286  80.18.0.10     C5/0/0/U0  online      2     0   264   N/A
0016.92fb.55be  80.18.0.7      C5/0/0/U0  online      3     0   288   N/A
0016.92f0.9104  80.18.0.5      C5/0/0/U0  online      4     0   280   N/A
0016.92fb.55c0  80.18.0.6      C5/0/0/U0  online      5     0   272   N/A
```

```
Router#
```

**Related Commands**

Command	Description
clear cable flap-list	Resets the flap-list table for a specific CM or for all CMs.
clear cable modem counters	Resets the flapping counters of a CM to zero.
clear cable modem delete	Removes one or more CMs from the internal address and routing tables.
<b>clear cable modem lock</b>	Resets the lock on one or more CMs.
<b>clear cable modem offline</b>	Removes all offline CMs from the internal address and routing tables, or clears all flap list counters for offline CMs.
show cable modem	Displays the current status for one or more CMs.

**hw-module reload**

To reload the software in and restart a Cisco 1-Gbps Wideband SPA, use the **hw-module reload** command in privileged EXEC mode.

**hw-module bay slot/subslot/bay reload**

**Syntax Description**

<b>bay slot/subslot/bay</b>	Reloads the SPA in the location specified by the <i>slot/subslot/bay</i> argument. The following are the valid values: <ul style="list-style-type: none"> <li>• <i>slot</i> = 1 to 3</li> <li>• <i>subslot</i> = 0 or 1 (0 is always specified)</li> <li>• <i>bay</i> = 0 (upper bay) or 1 (lower bay)</li> </ul>
-----------------------------	---

**Defaults**

No default behavior or values

**Command Modes**

Privileged EXEC

Command History	Release	Modification
	12.3(21)BC	This command was introduced for the Cisco uBR10012 universal broadband router.

**Usage Guidelines** The **hw-module reload** command reloads the software in and restarts a Cisco 1-Gbps Wideband SPA.

**Examples** The following example shows reloads the Cisco Wideband SPA in slot 1, subslot 0, bay 1.

```
Router# hw-module bay 1/0/1 reload
Router#
```

Related Commands	Command	Description
	hw-module shutdown	Shuts down a PRE1 module, line card, SIP, or SPA.

## hw-module shutdown

To shut down a particular Performance Routing Engine (PRE1) module, line card, Wideband SIP or Wideband SPA, use the **hw-module shutdown** command in global configuration mode. To activate a specific PRE1, line card, Wideband SIP or Wideband SPA, use the **no** form of this command.

```
hw-module {main-cpu | pre {A|B} | sec-cpu | slot slot-number | subslot slot/subslot | bay slot/subslot/bay} shutdown [unpowered]
```

```
no hw-module {main-cpu | pre {A|B} | sec-cpu | slot slot-number | subslot slot/subslot | bay slot/subslot/bay} shutdown
```

Syntax Description		
	<b>main-cpu</b>	Shuts down the PRE1 module that is currently acting as the active PRE1 module.
	<b>pre</b> {A B}	Shuts down the PRE1 module that is physically in either PRE slot A (left slot) or PRE slot B (right slot).
	<b>sec-cpu</b>	Shuts down the PRE1 module that is currently acting as the standby PRE1 module.
	<b>slot</b> <i>slot-number</i>	Shuts down the line cards that are physically present in the specified <i>slot-number</i> (valid range is 1 to 8).
	<b>subslot</b> <i>slot/subslot</i>	Shuts down the line card or SIP that is physically present in the slot with the specified slot and subslot numbers. The following are the valid values: <ul style="list-style-type: none"> <li><i>slot</i> = 1 to 8</li> <li><i>subslot</i> = 0 or 1</li> </ul>

<b>bay</b> <i>slot/subslot/bay</i>	Shuts down the SPA in the location specified by the <i>slot/subslot/bay</i> argument. The following are the valid values: <ul style="list-style-type: none"> <li>• <i>slot</i> = 1 to 3</li> <li>• <i>subslot</i> = 0 or 1 (0 is always specified)</li> <li>• <i>bay</i> = 0 (upper bay) or 1 (lower bay)</li> </ul>
unpowered	Used with the Wideband SPA, shuts down the SPA and its interfaces, and leaves them in an administratively down state without power.

**Defaults**

No default behavior or values

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
12.3(21)BC	Support was added for the Cisco Wideband SIP and Cisco 1-Gbps Wideband SPA.

**Usage Guidelines**

The **hw-module shutdown** command shuts down a particular Performance Routing Engine (PRE1) module, line card, Wideband SIP or Wideband SPA. To activate a specific PRE1, line card, Wideband SIP, or Wideband SPA, use the **no** form of this command.



**Caution**

Shutting down the active PRE1 module will trigger a switchover, so that the standby PRE1 module becomes the active PRE1 module.

**Examples**

The following example shows the standby PRE1 module being shut down:

```
Router(config)# hw-module sec-cpu shutdown
Router(config)#
```

The following example shows the active PRE1 module being shut down (which will trigger a switchover to the standby PRE1 module):

```
Router(config)# hw-module main-cpu shutdown
Router(config)#
```

The following example shows the PRE1 module in PRE1 slot B being shut down:

```
Router(config)# hw-module pre B shutdown
Router(config)#
```



**Note**

The **hw-module pre B shutdown** command shuts down the PRE1 module that is physically present in slot B, regardless of whether the module is the active or standby PRE1 module.

The following example shows how to deactivate and verify deactivation for the Cisco Wideband SPA located in slot 1, subslot 0, bay 0. In the output of the **show hw-module bay oir** command, notice the “admin down” in the Operational Status field.

```
Router# configure terminal
Router(config)# hw-module bay 1/0/0 shutdown unpowered
%SPAWBCMTS-4-SFP_MISSING: Wideband-Cable 1/0/0, 1000BASE-SX SFP missing from port 0
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:1, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:2, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:3, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:4, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:5, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:6, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:7, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:8, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:9, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:10, changed state to down
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:11, changed state to down
...
Router# show hw-module bay 1/0/0 oir
```

Module	Model	Operational Status
bay 1/0/0	SPA-24XDS-SFP	admin down

The following example shows how to activate and verify activation for the Cisco Wideband SPA located in slot 1, subslot 0, bay 0. In the output of the **show hw-module bay oir** command, notice the “ok” in the Operational Status field.

```
Router# configure terminal
Router(config)# no hw-module bay 1/0/0 shutdown
%SPAWBCMTS-4-SFP_OK: Wideband-Cable 1/0/0, 1000BASE-SX SFP inserted in port 0
%SPAWBCMTS-4-SFP_LINK_OK: Wideband-Cable 1/0/0, port 0 link changed state to up
%SNMP-5-LINK_UP: LinkUp:Interface Wideband-Cable1/0/0:0 changed state to up
%LINK-3-UPDOWN: Interface Cable1/0/0:0, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:1, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:2, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:3, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:4, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:5, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:6, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:7, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:8, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:9, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:10, changed state to up
%LINK-3-UPDOWN: Interface Wideband-Cable1/0/0:11, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Wideband-Cable1/0/0:0, changed state to up
...
Router# show hw-module bay 1/0/0 oir
```

Module	Model	Operational Status
bay 1/0/0	SPA-24XDS-SFP	ok

## Related Commands

Command	Description
hw-module reset	Resets a PRE1 module or line card.

Command	Description
hw-module-reload	Reloads the software in and restarts a Cisco 1-Gbps Wideband SPA.
redundancy force-failover main-cpu	Forces a manual switchover between the active and standby PRE1 modules.

## show cable modem summary

To display a summary of CMs on one or more cable interfaces, use the **show cable modem** command in privileged EXEC mode.

- show cable modem summary [total]**
- show cable modem summary interface1 [interface2] total**
- show cable modem summary interface1 [interface2] upstream port1 port2 total**
- show cable modem cable slot/port [upstream port] summary**
- show cable modem cable slot/subslot/port [upstream port] summary**

Syntax	Description
<b>total</b>	(Optional) Displays a footer line showing the totals for each column.
<b>interface1</b>	(Optional) Cable interface to be summarized. The <i>interface1</i> parameter can take the following forms: <ul style="list-style-type: none"> <li>• <b>cable slot/port</b>—On the Cisco uBR7100 series router, the only valid value is <b>1/0</b>. On the Cisco uBR7200 series router, <i>slot</i> can range from 3 to 6, and <i>port</i> can be 0 or 1, depending on the cable interface.</li> <li>• <b>cable slot/subslot/port</b>—On the Cisco uBR10012 router, <i>slot</i> can range from 5 to 8, <i>subslot</i> can be either 0 or 1, and <i>port</i> can range from 0 to 4 (depending on the interface).</li> </ul>
<b>interface2</b>	(Optional) Second cable interface, specifying a range of cable interfaces to be summarized. The <i>interface2</i> parameter has the same form as <i>interface1</i> . <p><b>Note</b> When specifying a range of cable interfaces, <i>interface1</i> must be the lower-numbered interface and <i>interface2</i> must be the higher-numbered interface.</p>
<b>upstream port1 port2</b>	(Optional) Specifies a range of upstream ports on the cable interfaces to be summarized. The <i>port1</i> and <i>port2</i> parameters can start at 0, and <i>port2</i> must be a higher-numbered port than <i>port1</i> .
<b>upstream port</b>	(Optional) Specifies a specific upstream port to be summarized. This option can be specified only when summarizing a single cable interface.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.3XA	This command was introduced.
	12.1(4)CX and 12.2(4)BC1	Support was added for the Cisco uBR10012 router.
	12.1(6)EC	The <b>total</b> option was supported for the Cisco uBR7100 series and Cisco uBR7200 series routers.
	12.1(11b)EC	The upstream Description field was added to the <b>show cable modem summary</b> display in Cisco IOS Release 12.1 EC.
	12.2(8)BC1	The <b>total</b> option was supported for the Cisco uBR10012 universal broadband router.
	12.2(15)BC2	The upstream Description field was added to the <b>show cable modem summary</b> display in Cisco IOS Release 12.2 BC.
	12.3(21)BC	Support was added for wideband modem output.

### Usage Guidelines

This command displays a summary of CMs for a single cable interface or upstream, or for a range of cable interfaces or upstreams. The following possible combinations are possible for this command:

- **show cable modem summary total**—Displays a summary and a total for all CMs on the chassis.
- **show cable modem summary cable x/0 total**—Displays a summary of CMs on a specified card.
- **show cable modem summary cable x/0 upstream port1 port2 total**—Displays a summary of CMs on the specified card and specified range of ports. The *port1* value must be less than the *port2* value.
- **show cable modem summary cable x/0 cable y/0 total**—Displays a summary of CMs on the specified range of cards.
- **show cable modem summary cable x/0 cable y/0 upstream port1 port2 total**—Displays a summary of CMs on the specified range of ports on the specified range of cards.



#### Note

Also see the information about this command's behavior in a Hot Standby Connection-to-Connection Protocol (HCCP) configuration, see the "Operation with Hot Standby Connection-to-Connection Protocol (HCCP) Configuration" section on page 3-63.

### Examples

The following example shows typical output for the default form of the **show cable modem summary** command on a Cisco uBR7200 series router:

```
Router# show cable modem summary

Interface      Total      Active      Registered  Description
              Modems    Modems
Cable3/0/U0    165        141         141         Line 32/1
Cable3/0/U1    209        172         170         Line 32/2
Cable3/0/U2    262        207         203         Line 32/3
Cable3/0/U3    256        194         188         Line 32/4
Cable5/0/U0    746        714         711         Line 41/1
Cable6/0/U0    806        764         759         Line 42/2

Router#
```



**Note**

The Description field appears in Cisco IOS Release 12.1(11b)EC, 12.2(15)BC2, and later releases, and shows the string configured for the upstream using the **cable upstream description** command.

The following example shows typical output for the **show cable modem summary** command with the **total** option on a Cisco uBR7200 series router:

```
Router# show cable modem summary total

Interface      Total      Active      Registered  Description
              Modems    Modems      Modems
Cable5/0/U0    746        714        711         Node1
Cable6/0/U1    806        764        759         Node3

Total:         1552      1478      1470
```

Router#

The following example shows sample output for the **show cable modem summary** command with the **total** option for a Cisco uBR10012 router:

```
Router# show cable modem summary total
Interface      Cable Modem      Description
              Total Reg  Unreg Offline Wideband initRC initD initIO initO
C5/0/0/U0     84   84   0   0     84     0   0   0   0
C5/0/0/U1     84   84   0   0     84     0   0   0   0
C5/0/0/U2     83   83   0   0     83     0   0   0   0
C5/0/0/U3     83   83   0   0     83     0   0   0   0
<<output omitted>>

Total:        8020 8020 0   0     8016   0   0   0   0
```

Router#

The following example shows sample output for the **show cable modem summary total** command for a range of interfaces on the Cisco uBR10012 router:

```
Router# show cable modem summary c5/1/1 c5/1/2 total
Interface      Cable Modem      Description
              Total Reg  Unreg Offline Wideband initRC initD initIO initO
C5/1/1/U0     84   84   0   0     84     0   0   0   0
C5/1/1/U1     84   84   0   0     83     0   0   0   0
C5/1/1/U2     83   83   0   0     83     0   0   0   0
C5/1/1/U3     83   83   0   0     83     0   0   0   0
C5/1/2/U0     84   84   0   0     84     0   0   0   0
C5/1/2/U1     84   84   0   0     84     0   0   0   0
C5/1/2/U2     83   83   0   0     83     0   0   0   0
C5/1/2/U3     83   83   0   0     83     0   0   0   0

Total:        668  668  0   0     667   0   0   0   0
```

Router#

The following example shows sample output for the **show cable modem summary total** command for a range of interfaces and upstreams on the Cisco uBR10012 router:

```
Router# show cable modem summary c5/1/1 c5/1/2 upstream 0 1 total
Interface      Cable Modem      Description
              Total Reg  Unreg Offline Wideband initRC initD initIO initO
C5/1/1/U0     84   84   0   0     84     0   0   0   0
C5/1/1/U1     84   84   0   0     83     0   0   0   0
C5/1/2/U0     84   84   0   0     84     0   0   0   0
```

```

C5/1/2/U1  84   84   0   0   84   0   0   0   0
Total:     336  336   0   0  335   0   0   0   0

```

Router#

**Note**

When displaying a summary for a range of ports or cable interfaces, the first port or cable interface (for example, u0 or c4/0) must be lower-numbered than the second port or interface (for example, u6 or c6/0). If you specify the higher-numbered port or interface first, the display shows no CMs connected.

Table 11 describes the fields shown in the **show cable modem summary** displays:

**Table 11** Descriptions for the **show cable modem summary** Fields

Field	Description
Interface	The cable interface line card providing the upstream for the CMs.
Total Modems or Total	Total number of CMs, registered, unregistered, and offline for this interface.
Registered Modems or Reg	Total number of CMs that have registered and are online on this interface. This number might be different from the Total Modems number if some modems are offline or not fully registered.
Unregistered Modems	Total number of CMs that are either offline and not currently communicating with the CMTS, or attempting to come online but are not yet registered.
Offline	Total number of CMs that were online or attempted to register but are no longer communicating with the CMTS.
Wideband	CM is registered as a wideband CM.
init(rc)	MAC state of CM is init(rc).
init(d)	MAC state of CM is init(d).
init(io)	MAC state of CM is init(io).
init(o)	MAC state of CM is init(o).
Description	Description entered for this upstream using the <b>cable upstream description</b> command.

**Note**

For information on MAC states, see the **show cable modem** command.

**Tip**

In Cisco IOS Release 12.1(12)EC, Release 12.2(8)BC1, and later releases, you can add a timestamp to **show** commands using the **exec prompt timestamp** command in line configuration mode.

**Related Commands**

Command	Description
<b>show cable modem</b>	Displays information for the registered and unregistered CMs.
<b>show cable modem access-group</b>	Displays the access groups for the CMs on a particular cable interface.

Command	Description
show cable modem calls	Displays voice call information for a particular CM, identified either by its IP address or MAC address.
show cable modem connectivity	Displays connectivity statistics for one or more CMs.
show cable modem counters	Displays downstream and upstream traffic counters for one or more CMs.
show cable modem cpe	Displays the CPE devices accessing the cable interface through a particular CM.
show cable modem offline	Displays a list of the CMs that are marked as offline with the Cisco CMTS.
show cable modem registered	Displays a list of the CMs that are marked as registered with the Cisco CMTS.
show cable modem remote-query	Displays information collected by the remote-query feature.
show cable modem unregistered	Displays a list of the CMs that are marked as unregistered with the Cisco CMTS.
show cable modem vendor	Displays the vendor name or Organizational Unique Identifier (OUI) for the CMs on each cable interface.
show interface cable modem	Displays information about the CMs connected to a particular cable interface.
show interface cable sid	Displays cable interface information.
show cable modem wideband	Displays information for a wideband CMs.

## show cable modem wideband

To display information for registered and unregistered wideband CMs, use the **show cable modem wideband** command in privileged EXEC mode.

**show cable modem wideband [registered-traditional-docsis]**

**show cable modem [ip-address | mac-address | cable slot/subslot/port] wideband**

### Syntax Description

ip-address	(Optional) Identifies the IP address of a specific wideband CM to be displayed. If you specify the IP address for a CPE device behind a CM, information for that CM is displayed.
mac-address	(Optional) Identifies the MAC address of a specific wideband CM to be displayed. You can also specify the MAC address for a CPE device behind a wideband CM, and information for that wideband CM will be displayed.

<code>cable slot/subslot/port</code>	(Optional) Identifies a cable interface on the Cisco uBR10012 router. The following are the valid values: <ul style="list-style-type: none"> <li><code>slot = 5 to 8</code></li> <li><code>subslot = 0 or 1</code></li> <li><code>port = 0 to 4</code> (depending on the cable interface)</li> </ul>
<code>registered-traditional-docsis</code>	(Optional) Displays information for wideband CMs that are currently registered as traditional DOCSIS modems.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(21)BC	This command was introduced for the Cisco uBR10012 universal broadband router.

**Usage Guidelines** This command displays information for a one or more wideband CMs. Optionally, the CMs for which to display information can be identified IP address, MAC address, or cable interface.

If a wideband-capable CM is not able to register as a wideband CM (for example, if no wideband channel is available), the CM attempts to register as a traditional DOCSIS modem. The **registered-traditional-docsis** keyword limits the set of wideband CMs for which to display information to wideband-capable CMs that are currently registered as DOCSIS 1.X or DOCSIS 2.0 modems.

**Examples** The following example shows typical output for the default form of the **show cable modem wideband** command on a Cisco uBR10012 router:

```
Router# show cable modem wideband
MAC Address      IP Address      I/F           MAC           Prim  BGDSID MD-DS-SG
                  State           ID
0014.bfbe.3cc0  1.11.0.1       C5/0/1/U0    w-online(pt)  3     24     24    N/A
0016.92f0.90d6  1.11.0.4       C5/0/1/U0    w-online(pt)  5     24     272   1
0014.bfbe.3cb8  1.11.0.2       C6/0/1/U0    w-online(pt)  3     36     36    N/A
0016.92f0.90d8  1.11.0.3       C6/0/1/U0    w-online(pt)  5     36     274   1
```

Router#

Table 12 describes the fields that are shown in the **show cable modem wideband** display:

**Table 12** Descriptions for the **show cable modem wideband** Fields

Field	Description
MAC Address	The MAC address for the CM.
IP Address	The IP address that the DHCP server has assigned to the CM.
I/F	The cable interface providing the upstream for this CM.
MAC State	The current state of the MAC layer.
Prim SID	The primary SID assigned to this CM.

**Table 12** Descriptions for the show cable modem wideband Fields (continued)

Field	Description
Bonding Group ID	The identifier of the primary wideband channel.
DSID	The Downstream Service Identifier.
MD-DS-SG	The MAC Domain Downstream Service Group, the downstream channels of a single MAC domain that reach the cable modem.

Table 13 shows the possible values for the MAC State field for a wideband CM modem that registers as a traditional DOCSIS modem:

**Table 13** Descriptions for the MAC State Field (for Traditional DOCSIS Modems) <sup>1</sup>

MAC State Value	Description
<b>Registration and Provisioning Status Conditions</b>	
init(r1)	The CM sent initial ranging.
init(r2)	The CM is ranging. The CMTS received initial ranging from the CM and has sent RF power, timing offset, and frequency adjustments to the CM.
init(rc)	Ranging has completed.  <b>Note</b> If a CM appears to be stuck in this state, it could be that the CM is able to communicate successfully on the cable network, but that the upstream is at capacity and does not have any additional bandwidth to allow the CM to finish registration and come online. Either manually move one or more CMs to other upstreams, or enable load balancing on the upstream using the <b>cable load-balance group</b> commands.
init(d)	The DHCP request was received, as DHCPDISCOVER. This also indicates that the first IP broadcast packet has been received from the CM.
init(dr)	The DHCP request has been sent to the cable modem.
init(i)	The cable modem has received the DHCPOFFER reply (DHCPACK) from the DHCP server that has assigned an IP address to the modem, but the modem has not yet replied with a DHCPREQUEST message requesting that particular IP address, nor has it sent an IP packet with that IP address.  <b>Note</b> If a CM appears to be stuck in this state, the CM has likely received the DHCPOFFER reply from the DHCP server, but this reply might have contained one or more invalid options for that particular CM.
init(io)	The Cisco CMTS has seen the DHCP offer as sent to the cable modem from the DHCP server that has assigned an IP address to the modem.
init(o)	The CM has begun to download the option file (DOCSIS configuration file) using the Trivial File Transfer Protocol (TFTP), as specified in the DHCP response. If the CM remains in this state, it indicates that the download has failed.
init(t)	Time-of-day (TOD) exchange has started.
resetting	The CM is being reset and will shortly restart the registration process.

**Table 13** Descriptions for the MAC State Field (for Traditional DOCSIS Modems) <sup>1</sup> (continued)

MAC State Value	Description
<b>Non-error Status Conditions</b>	
cc(r1)	The CM had registered and was online, but has received a Downstream Channel Change (DCC) or Upstream Channel Change (UCC) request message from the CMTS. The CM has begun moving to the new channel, and the CMTS has received the CM's initial ranging on the new downstream or upstream channel. At the MAC layer, the CM is considered offline because it is not yet passing traffic on the new channel, but this state does not trigger the flap-list counters.
cc(r2)	This state should normally follow cc(r1) and indicates that the CM has finished its initial ranging on the new channel, and is currently performing continuous ranging on the new channel. At the MAC layer, the CM is considered offline because it is not yet passing traffic on the new channel, but this state does not trigger the flap-list counters.
offline	The CM is considered offline (disconnected or powered down).
online	The CM has registered and is enabled to pass data on the network.
online(d)	The CM registered, but network access for CPE devices using this CM has been disabled through the DOCSIS configuration file. The CM does not forward traffic to or from the CPE devices, but the CMTS can continue to communicate with the CM using DOCSIS messages and IP traffic (such as SNMP commands).  <b>Note</b> If BPI was enabled in the DOCSIS configuration file sent to the CM, assume that the CM is using BPI encryption, unless other messages show that the BPI negotiation and key assignments have failed.
online(pkd)	The CM registered, but network access for CPE devices using this CM has been disabled through the DOCSIS configuration file. In addition, BPI is enabled and KEK is assigned.  <b>Note</b> This state is equivalent to the online(d) and online(pk) states.
online(ptd)	The CM registered, but network access for CPE devices using this CM has been disabled through the DOCSIS configuration file. In addition, BPI is enabled and TEK is assigned. BPI encryption is now being performed.  <b>Note</b> This state is equivalent to the online(d) and online(pt) states.
online(pk)	The CM registered, BPI is enabled and KEK is assigned.
online(pt)	The CM registered, BPI is enabled and TEK is assigned. BPI encryption is now being performed.  <b>Note</b> If network access was disabled in the DOCSIS configuration file sent to the CM, the network disabled status takes precedence, and the MAC status field shows online(d) instead of online(pt) even when BPI encryption is enabled and operational.
<b>Note</b>	If an exclamation point (!) appears in front of one of the online states, it indicates that the <b>cable dynamic-secret</b> command has been used with either the <b>mark</b> or <b>reject</b> option, and that the cable modem has failed the dynamic secret authentication check.
expire(pk)	The CM registered, BPI is enabled, KEK was assigned, but the current KEK expired before the CM could successfully renew a new KEK value.

**Table 13** Descriptions for the MAC State Field (for Traditional DOCSIS Modems) <sup>1</sup> (continued)

MAC State Value	Description
expire(pkd)	<p>The CM registered, but network access for CPE devices using this CM has been disabled through the DOCSIS configuration file. In addition, BPI is enabled, KEK was assigned, but the current KEK expired before the CM could successfully renew a new KEK value.</p> <p><b>Note</b> This state is equivalent to the online(d) and expire(pk) states.</p>
expire(pt)	<p>The CM registered, BPI is enabled, TEK was assigned, but the current TEK expired before the CM could successfully renew a new KEK value.</p>
expire(ptd)	<p>The CM registered, but network access for CPE devices using this CM has been disabled through the DOCSIS configuration file. In addition, BPI is enabled, TEK was assigned, but the current TEK expired before the CM could successfully renew a new KEK value.</p> <p><b>Note</b> This state is equivalent to the online(d) and expire(pt) states.</p>
<b>Error Status Conditions</b>	
reject(m)	<p>The CM attempted to register but registration was refused due to a bad Message Integrity Check (MIC) value. This also could indicate that the shared secret in the DOCSIS configuration file does not match the value configured on the CMTS with the <b>cable shared-secret</b> command.</p> <p>In Cisco IOS Release 12.1(11b)EC1 and Cisco IOS Release 12.2(8)BC2 or later releases, this could also indicate that the <b>cable tftp-enforce</b> command has been used to require that a CM attempt a TFTP download of the DOCSIS configuration file before registering, but the CM did not do so.</p>
reject(c)	<p>The CM attempted to register, but registration was refused due to a number of possible errors:</p> <ul style="list-style-type: none"> <li>• The CM attempted to register with a minimum guaranteed upstream bandwidth that would exceed the limits imposed by the <b>cable upstream admission-control</b> command.</li> <li>• The CM has been disabled because of a security violation.</li> <li>• A bad class of service (COS) value in the DOCSIS configuration file.</li> <li>• The CM attempted to create a new COS configuration but the CMTS is configured to not permit such changes.</li> <li>• The CM failed the timestamp check for its DOCSIS configuration file. (This could indicate a possible theft-of-service attempt, or a problem with the synchronization of the clocks on the CM and CMTS.)</li> </ul>
reject(pk)	<p>KEK key assignment is rejected, BPI encryption has not been established.</p>
reject(pkd)	<p>The CM registered, but network access for CPE devices using this CM has been disabled through the DOCSIS configuration file. In addition, BPI encryption was not established because KEK key assignment was rejected.</p> <p><b>Note</b> This state is equivalent to the online(d) and reject(pk) states.</p>
reject(pt)	<p>TEK key assignment is rejected, BPI encryption has not been established.</p>

**Table 13** Descriptions for the MAC State Field (for Traditional DOCSIS Modems) <sup>1</sup> (continued)

MAC State Value	Description
reject(ptd)	The CM registered, but network access for CPE devices using this CM has been disabled through the DOCSIS configuration file. In addition, BPI encryption was not established because TEK key assignment was rejected.  <b>Note</b> This state is equivalent to the online(d) and reject(pt) states.
reject(ts)	The CM attempted to register, but registration failed because the TFTP server timestamp in the CM registration request did not match the timestamp maintained by the CMTS. This might indicate that the CM attempted to register by replaying an old DOCSIS configuration file used during a prior registration attempt.
reject(ip)	The CM attempted to register, but registration failed because the IP address in the CM request did not match the IP address that the TFTP server recorded when it sent the DOCSIS configuration file to the CM. IP spoofing could be occurring.
reject(na)	The CM attempted to register, but registration failed because the CM did not send a Registration-Acknowledgement (REG-ACK) message in reply to the Registration-Response (REG-RSP) message sent by the CMTS. A Registration-NonAcknowledgement (REG-NACK) is assumed.

1. The CM MAC state field can also be retrieved using SNMP by getting the value of the cdxCmtsCmStatusValue object in the CISCO-DOCS-EXT-MIB.

**Tip**

In Cisco IOS Release 12.1(12)EC, Release 12.2(8)BC1, and later releases, you can add a timestamp to **show** commands using the **exec prompt timestamp** command in line configuration mode.

Table 14 shows the possible values for the MAC state field for a wideband-capable CM that registers as a wideband modem:

**Table 14** Additional MAC States for a Wideband Cable Modem

MAC State Value	Description
<b>Non-error Status Conditions</b>	
w-online	The WCM has registered and is enabled to pass data on the network.
w-online(d)	The WCM registered, but network access for CPE devices using this WCM has been disabled through the DOCSIS configuration file. The CM does not forward traffic to or from the CPE devices, but the WCMTS can continue to communicate with the WCM using DOCSIS messages and IP traffic (such as SNMP commands).  <b>Note</b> If BPI was enabled in the DOCSIS configuration file sent to the WCM, assume that the CM is using BPI encryption, unless other messages show that the BPI negotiation and key assignments have failed.
w-online(pkd)	The WCM registered, but network access for CPE devices using this WCM has been disabled through the DOCSIS configuration file. In addition, BPI is enabled and KEK is assigned.  <b>Note</b> This state is equivalent to the w-online(d) and w-online(pk) states.

**Table 14 Additional MAC States for a Wideband Cable Modem (continued)**

MAC State Value	Description
w-online(pt)	The WCM registered, BPI is enabled and TEK is assigned. BPI encryption is now being performed. <b>Note</b> If network access was disabled in the DOCSIS configuration file sent to the WCM, the network disabled status takes precedence, and the MAC status field shows w-online(d) instead of w-online(pt) even when BPI encryption is enabled and operational.
w-online(ptd)	The WCM registered, but network access for CPE devices using this WCM has been disabled through the DOCSIS configuration file. In addition, BPI is enabled and TEK is assigned. BPI encryption is now being performed. <b>Note</b> This state is equivalent to the w-online(d) and w-online(pt) states.
w-online(pk)	The WCM registered, BPI is enabled and KEK is assigned.
w-expire(pk)	The WCM registered, BPI is enabled, KEK was assigned, but the current KEK expired before the WCM could successfully renew a new KEK value.
w-expire(pkd)	The WCM registered, but network access for CPE devices using this WCM has been disabled through the DOCSIS configuration file. In addition, BPI is enabled, KEK was assigned, but the current KEK expired before the CM could successfully renew a new KEK value. <b>Note</b> This state is equivalent to the w-online(d) and w-expire(pk) states.
w-expire(pt)	The WCM registered, BPI is enabled, TEK was assigned, but the current TEK expired before the WCM could successfully renew a new KEK value.
w-expire(ptd)	The WCM registered, but network access for CPE devices using this WCM has been disabled through the DOCSIS configuration file. In addition, BPI is enabled, TEK was assigned, but the current TEK expired before the WCM could successfully renew a new KEK value. <b>Note</b> This state is equivalent to the w-online(d) and w-expire(pt) states.
<b>Error Status Conditions</b>	
w-reject(pk)	KEK key assignment is rejected, BPI encryption has not been established.
w-reject(pkd)	The WCM registered, but network access for CPE devices using this WCM has been disabled through the DOCSIS configuration file. In addition, BPI encryption was not established because KEK key assignment was rejected. <b>Note</b> This state is equivalent to the w-online(d) and w-reject(pk) states.
w-reject(pt)	TEK key assignment is rejected, BPI encryption has not been established.
w-reject(ptd)	The WCM registered, but network access for CPE devices using this WCM has been disabled through the DOCSIS configuration file. In addition, BPI encryption was not established because TEK key assignment was rejected. <b>Note</b> This state is equivalent to the w-online(d) and w-reject(pt) states.

**Related Commands**

Command	Description
show cable modem vendor	Associates the name of a vendor with its Organizational Unique Identifier (OUI).
<b>show cable modem</b>	Displays information for the registered and unregistered CMs.

Command	Description
<b>show cable modem summary</b>	Displays displays voice call information for a particular CM, identified either by its IP address or MAC address.
<b>show cable modem classifiers</b>	Displays information about the classifiers for a particular CM.
<b>show cable modem cnr</b>	Displays information about the upstream carrier-to-noise ratio (CNR) for a particular cable modem.
<b>show cable modem connectivity</b>	Displays connectivity statistics for one or more CMs.
<b>show cable modem errors</b>	Displays error statistics for one or more CMs.
<b>show cable modem flap</b>	Displays flap list statistics for one or more cable modems.
<b>show cable modem maintenance</b>	Displays station maintenance (SM) error statistics for one or more cable modems.
<b>show cable modem remote-query</b>	Displays information collected by the remote-query feature.
<b>show cable modulation-profile</b>	Displays modulation profile group information.
<b>show interface cable modem</b>	Displays information about the CMs connected to a particular cable interface.
<b>show interface cable sid</b>	Displays cable interface information.

## show interface wideband-cable

To display the current configuration and status for a wideband channel, use the **show interface wideband-cable** command in privileged EXEC mode.

```
show interface wideband-cable slot/subslot/bay:wideband_channel [options]
```

**Syntax Description**

slot/subslot/bay:wideband-channel Identifies a Wideband SIP and SPA on the Cisco uBR10012 router and the wideband channel number. The following are the valid values:

- slot = 1 to 3
- subslot = 0 or 1 (always 0)
- bay = 0 (upper bay) or 1 (lower bay)
- wideband-channel = 0 to 11

options The following non-cable specific options generate information for wideband cable interfaces:

- accounting**—Displays the number of packets of each protocol type that was sent through the interface.
- description**—Displays the description entered for the interface.
- privacy**—Displays privacy group information.
- stats**—Displays packets that were switched.
- summary**—Displays interface summary information.
- switching**—Displays interface switching information.

**Note** Some other non-cable specific options do not generate any meaningful information for wideband cable interfaces.



**Note**

For information on the non-cable specific options, see the Cisco IOS Release 12.3 documentation on [Cisco.com](http://Cisco.com) and the Customer Documentation CD-ROM.

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
12.3(21)BC	This command was introduced on the uBR10012 universal broadband router.

**Examples**

The following is a sample output for the **show interface wideband-cable** command:

```
Router# show interface wideband-cable 1/0/0:1

Wideband-Cable1/0/0:1 is up, line protocol is up
  Hardware is Wideband CMTS Cable interface, address is 0012.001a.8897 (bia
0012.001a.8897)
  MTU 1500 bytes, BW 74730 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation MCNS, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```

Output queue: 0/40 (size/max)
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  24224 packets output, 1222002 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out

```

Router#

Table 15 describes the fields shown in the **show interface wideband-cable** display.

**Table 15** *show interface wideband-cable Field Descriptions*

Field	Description
Wideband-Cable slot/subslot/bay:wb-channel is up/...administratively down	Indicates whether the interface hardware is currently active or taken down by the administrator.
line protocol is up/...administratively down	Indicates whether the software processes that handle the line protocol believe the interface is usable or if it has been taken down by the administrator.
hardware	Hardware type and address.
Internet address	Internet address followed by subnet mask.
MTU	Maximum transmission unit (MTU) of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255, calculated as an exponential average over 5 minutes. (For example, 255/255 is 100 percent reliability.)
load	Load on the interface as a fraction of 255, calculated as an exponential average over 5 minutes. (For example, 255/255 is complete saturation.)
Encapsulation	Encapsulation method assigned to this interface.
Keepalive set	Keepalive time interval.
ARP type	Type of Address Resolution Protocol (ARP) and timeout value assigned.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface.
output	Number of hours, minutes, and seconds since the last packet was successfully sent by an interface.
Last clearing of "show interface" counters	Time at which the counters that measure cumulative statistics (such as number of bytes sent and received) were last reset to zero.
Queueing strategy	Displays the type of queueing configured for this interface. In the following example output, the type of queueing configured is first-in first-out (FIFO).

**Table 15** *show interface wideband-cable Field Descriptions (continued)*

Field	Description
Output queue	Number of packets in the output queue. The format of this number is A/B, where A indicates the number of packets in the queue, and B indicates the maximum number of packets allowed in the queue.
drops	Indicates the number of packets dropped because of a full queue.
input queue/drops	Number of packets in the input queue. The format of this number is A/B, where A indicates the number of packets in the queue, and B indicates the maximum number of packets allowed in the queue.
drops	Indicates the number of packets dropped because of a full queue.
Five minute input rate Five minute output rate	Average number of bits and packets sent per second in the last five minutes. The five-minute interval is the default time period for statistics collection and can be changed for each individual cable interface using the <b>load-interval</b> command in interface configuration mode.

**Note** These statistics are calculated using a decayed averaging method, where only the average is stored over the interval period, not the individual samples. Every time a sample average is taken, a percentage of the sample and a percentage of the average are added together to create the new average. If traffic stops for a time period, these statistics do not immediately go to zero but drop with a decay rate of about 70 percent per time period.

For example, if the interface is passing 1,000 packets per second (pps) before traffic stops, the **show interface cable** command shows the rate being 300 pps at the end of the first time interval. The rate then drops to 90 pps at the end of the second time interval, and so forth.

packets input	Total number of error-free packets received by the system.
bytes input	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system.
Received broadcast	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they are bigger than the standard Ethernet Maximum Transmission Unit (MTU) size. For Ethernet packets, RFC 1757 defines giants as "the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed."
	<b>Note</b> In addition, to account for the different Ethernet and other packet encapsulations on the network, packets are considered giants when they exceed the configured MTU size plus 114 bytes.

**Table 15** *show interface wideband-cable Field Descriptions (continued)*

Field	Description
input errors	Total number of errors received on the interface. This count includes runts and giants, which are shown above, as well as other errors, such as no buffers, and CRC, frame, overrun, and ignored counts. This count can also include DOCSIS protocol errors such as an invalid SID in the DOCSIS frame, a bad extended header length, corrupted concatenated packets, and invalid bandwidth requests.
CRC	Indicates the number of times the cyclic redundancy checksum (CRC) generated by the originating LAN station or far-end device does not match the checksum calculated from the data received.
frame	Number of packets received incorrectly having a CRC error and a non-integer number of octets.
overrun	Number of times the receiver hardware was unable to forward received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers.
packets output	Total number of messages sent by the system.
bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
underruns	Number of times the sender has been running faster than the receiving device can handle.
output errors	Sum of all errors that prevented the final transmission of packets out of the interface being examined.
collisions	Not applicable.
interface resets	Number of times an interface has been completely reset.
output buffer failures	Number of times the output buffer has failed.
output buffer swapped out	Number of times the output buffer has been swapped out.

**Tip**

In Cisco IOS Release 12.1(12)EC, Release 12.2(8)BC1, and later releases, you can add a timestamp to **show** commands using the **exec prompt timestamp** command in line configuration mode.

**Related Commands**

Command	Description
<b>show interface cable downstream</b>	Displays information about the downstream on the cable interface.
<b>show interface cable sid</b>	Displays information by service identifier (SID) of each CM on the network.

Command	Description
<b>show interface cable signal-quality</b>	Displays information about the cable signal quality.
<b>show interface cable upstream</b>	Displays information about one or all upstreams on the cable interface.

## Restrictions for Cisco IOS Release 12.3(17a)BC

When upgrading the Cisco uBR10012 Performance Routing Engine 1 (PRE1) modules to Cisco uBR10012 PRE2 modules, you must reconfigure the cable intercept feature when enabled on a slave interface. For additional information about the Cable Intercept feature, cable interface bundling, or virtual master interfaces in cable interface bundling, refer to the following documents on Cisco.com:

- *Cable Interface Bundling and Virtual Interface Bundling for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_bund.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_bund.html)
- *Cable Monitor and Intercept Features for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cmon.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html)
- *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## New Command Information for Cisco IOS Release 12.3(13a)BC3

Cisco IOS Release 12.3(13a)BC3 introduces support for the **debug cable classifier** command, which displays debugging information supporting DOCSIS packet classifiers.

### debug cable classifiers

To display debugging messages for DOCSIS packet classifiers, use the **debug cable classifiers** command in privileged EXEC mode. To stop the display of debugging messages, use the **no** form of this command.

- debug cable classifiers**
- no debug cable classifiers**

**Syntax Description** No additional keywords or syntax components are required.

**Command Modes** Privileged EXEC mode

**Defaults** DOCSIS packet classifier debugging is disabled by default.

**Command History**

Release	Modification
12.3(13a)BC3	This command was introduced on the Cisco uBR10012 and Cisco uBR7246VXR universal broadband routers.

**Usage Guidelines**

The **debug cable classifiers** command provides detailed information about the allocation, removal, activation and deactivation of packet classifiers. Generally, classifiers are used to identify IP packets by source port, destination port, or type of service. Classifiers are associated with service flows. For example, packet classifiers are dynamically created in most Voice over IP (VoIP) deployments and this debug command can be used to troubleshoot issues related to these classifiers as VOIP calls are created and torn down.

Because this command can produce a large volume of debug information, use this command only when you have also enabled debugging for a particular MAC address, set of MAC addresses, or a MAC address mask, using the **debug cable mac-address** command.

For additional debug command information, refer to the following document on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference*

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

**Examples**

The following example enables classifier debugging for a single MAC address:

```
Router# debug cable mac-address 000a.73fa.dbaa
Router# debug cable classifiers
CMTS Packet Classifiers debugging is on
```

The following enables classifier debugging for all MAC addresses with Organizational Unique Identifier (OUI) OUI 0013.11:

```
Router# debug cable mac-addr 0013.1100.0000 ffff.ff00.0000
Routerv# debug cable classifiers
CMTS Packet Classifiers debugging is on
```

The following example illustrates sample output of the **debug cable classifiers** command for the given MAC addresses:

```
Feb 7 18:43:50.181: CFR cmts_deactivate_us_srv_flow_act_cfrs 000a.73fa.dbaa sid 1 sfid 3
st 2 dir 0 prov 1 adm 1 act 1
Feb 7 18:43:50.181: CFR cmts_remove_cm_srv_flow_cfrs 000a.73fa.dbaa sid 1 sfid 3 st 2 dir
0 prov 1 adm 0 act 0
Feb 7 18:43:50.181: CFR cmts_deactivate_ds_srv_flow_act_cfrs 000a.73fa.dbaa sid 0 sfid 4
st 2 dir 1 prov 2 adm 2 act 2
Feb 7 18:43:50.181: CFR cmts_remove_cm_srv_flow_cfrs 000a.73fa.dbaa sid 0 sfid 4 st 2 dir
1 prov 2 adm 0 act 0
Feb 7 18:43:50.181: CFR cmts_deactivate_us_srv_flow_act_cfrs 000a.73fa.dbaa sid 1 sfid 3
st 2 dir 0 prov 3 adm 0 act 0
Feb 7 18:43:50.181: CFR cmts_deactivate_us_srv_flow_act_cfrs 000a.73fa.dbaa sid 1 sfid 3
st 1 dir 0 prov 3 adm 3 act 0
Feb 7 18:43:50.181: CFR cmts_activate_us_srv_flow_act_cfrs 000a.73fa.dbaa sid 1 sfid 3 st
2 dir 0 prov 3 adm 3 act 3
Feb 7 18:43:50.181: CFR cmts_deactivate_ds_srv_flow_act_cfrs 000a.73fa.dbaa sid 0 sfid 4
st 2 dir 1 prov 4 adm 0 act 0
Feb 7 18:43:50.181: CFR cmts_deactivate_ds_srv_flow_act_cfrs 000a.73fa.dbaa sid 0 sfid 4
st 1 dir 1 prov 4 adm 4 act 0
Feb 7 18:43:50.181: CFR cmts_activate_ds_srv_flow_act_cfrs 000a.73fa.dbaa sid 0 sfid 4 st
2 dir 1 prov 4 adm 4 act 4
Feb 7 18:43:50.181: CFR cmts_set_cfr_params 000a.73fa.dbaa cfrid 1 pri 0 ord 0 dir 0 st 2
phsi 0
Feb 7 18:43:50.181: CFR cmts_activate_cfr 000a.73fa.dbaa cfrid 1 pri 1 ord 0 dir 0 st 2
```

```
Feb 7 18:43:50.181: CFR cmts_add_pkt_cfr 000a.73fa.dbaa cfrid 1 pri 1 ord 0 dir 0 st 1
phsi 0
Feb 7 18:43:50.181: CFR cmts_handle_cfr_parsed_data CFR_ADD 000a.73fa.dbaa sfid 0 action
0 dir 0 type 0 cfrid 0 pri 1 ord 0 dir 0 st 1 phsi 0
Feb 7 18:43:50.181: CFR cmts_set_cfr_params 000a.73fa.dbaa cfrid 2 pri 0 ord 0 dir 1 st 2
phsi 0
Feb 7 18:43:50.181: CFR cmts_activate_cfr 000a.73fa.dbaa cfrid 2 pri 1 ord 0 dir 1 st 2
Feb 7 18:43:50.181: CFR cmts_add_pkt_cfr 000a.73fa.dbaa cfrid 2 pri 1 ord 1 dir 1 st 1
phsi 0
Feb 7 18:43:50.181: CFR cmts_handle_cfr_parsed_data CFR_ADD 000a.73fa.dbaa sfid 0 action
0 dir 1 typ
```

**Related Commands**

Command	Description
<b>debug cable dynsrv</b>	Displays information about DOCSIS 1.1 dynamic service flow messages.
<b>debug cable qos</b>	Activates quality-of-service (QoS) debugging.

## New Command Information for Cisco IOS Release 12.3(13a)BC2

Cisco IOS Release 12.3(13a)BC2 introduces support for the **cable service flow activity-timeout** command, which enables the configuration of dynamic service flow timeout settings apart from a PacketCable environment.

### cable service flow activity-timeout

To configure the activity timeout for dynamic cable service flows in DOCSIS 1.1 environments, where PacketCable is inactive, use the **cable service flow activity-timeout** command in global configuration mode. To remove the activity timer once configured, use the **no** form of this command.

- cable service flow activity-timeout** *n*
- no cable service flow activity-timeout** [*<n>*]

**Syntax Description**

<i>n</i>	The timeout length in seconds. Valid range is 0 - 65535 seconds. Setting this value to 0 configures the service flow to never timeout.
----------	--

**Defaults**

The default timeout length for a DOCSIS 1.0+ cable service flow is 300 seconds (five minutes).

**Command Modes**

Global configuration

**Command History**

Release	Modification
12.3(13a)BC	This command was introduced to support DOCSIS 1.1 service flow operation in non-Packet-Cable environments.

**Usage Guidelines**

Dynamic service flows in DOCSIS 1.0+ are created with a default activity timeout of 300 seconds. This enables the deletion of idle service flows after five minutes. This new command enables such functions within DOCSIS 1.1 environments with a wide range of timeout length options.

In DOCSIS 1.1, the default inactivity timeout is often set by the application that triggers the creation of dynamic service flows. PacketCable frequently performs this function when supported on the Cisco CMTS. However, this new command configures inactivity timeout where PacketCable is not active on the Cisco CMTS.

**Note**

When PacketCable is supported, PacketCable sets the inactivity timeout from the PacketCable gate, and the PacketCable activity overrides timeout values set with this command. This is the case even where the inactivity timeout is set to zero, which configures the service flow to never timeout.

Apart from PacketCable, this command enables the cable modem to control the setup of the dynamic service flows, and to remove inactive service flows. During the creation of service flows, all Upstream and Downstream flows in the request are checked to see if the configured activity timeout needs to be applied.

**Examples**

The following example in global configuration mode configures the cable modems connected to the Cisco CMTS to use activity timeout of zero, which means that related service flows do not timeout in a non-PacketCable environment:

```
Router(config)# cable service flow activity-timeout 0
```

**Related Commands**

Command	Description
cable qos profile	Creates a DOCSIS 1.0 QoS profile.
<b>cable service flow inactivity-threshold</b>	Sets the amount of time a dynamic service-flow can be present in the system without any activity (DOCSIS 1.1 operation).
<b>cable service-flow inactivity-timeout</b>	Sets the amount of time a dynamic service-flow can be present in the system without any activity (DOCSIS 1.0 operation).
<b>show cable service-class</b>	Displays the service classes that have been created.

## Restrictions for Cisco IOS Release 12.3(13a)BC

The following restrictions apply to Cisco IOS Release 12.3(13a)BC:

- Cisco IOS Release 12.3(13a)BC with the Cisco uBR10012 router does not support overlapping IP addresses with MPLS-VPN.
- When upgrading the Cisco uBR10012 Performance Routing Engine 1 (PRE1) modules to Cisco uBR10012 PRE2 modules, you must reconfigure the cable intercept feature when enabled on a slave interface. For additional information about the Cable Intercept feature, cable interface bundling, or virtual master interfaces in cable interface bundling, refer to the following documents on Cisco.com:
  - “Virtual Interface Bundling on the Cisco uBR10-MC5X20S/U BPE” section on page 90
  - *Cable Monitor and Intercept Features for the Cisco CMTS*  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cmon.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html)
  - *Cisco IOS CMTS Cable Command Reference*  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## Restrictions for Cisco IOS Release 12.3(9a)BC

The following restrictions apply to Cisco IOS Release 12.3(9a)BC:

- Cisco IOS Release 12.3(9a)BC with the Cisco uBR10012 router does not support overlapping IP addresses with MPLS-VPN.
- When upgrading the Cisco uBR10012 Performance Routing Engine 1 (PRE1) modules to Cisco uBR10012 PRE2 modules, you must reconfigure the cable intercept feature when enabled on a slave interface. For additional information about the Cable Intercept feature or cable interface bundling, refer to the following documents on Cisco.com:
  - Cable Monitor and Intercept Features for the Cisco CMTS  
[http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg\\_cmon.html](http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_cmon.html)
  - Cisco IOS CMTS Cable Command Reference  
[http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl\\_book.html](http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html)

## New and Changed Command Reference for Cisco IOS Release 12.3(9a)BC

Cisco IOS Release 12.3(9a)BC introduces or enhances the following Cisco IOS commands for the Cisco uBR10012 router:

- [cable logging layer2events](#)
- [cable source-verify](#)
- [cable submgmt default](#)
- [show cable tech-support](#)
- [show controllers cable](#)
- [show tech-support](#)

## cable logging layer2events

To save selected (low priority) DOCSIS events that are specified in CMTS MIB Registry to the cable logging buffer (instead of to the general logging buffer), use the **cable logging layer2events** command in global configuration mode. To disable the logging of DOCSIS events to the cable logging buffer, use the **no** form of this command.

**cable logging layer2events**

**no cable logging layer2events**

**Syntax Description** This command has no additional arguments or keywords.

**Defaults** DOCSIS events are saved to the general logging buffer on the Cisco CMTS by default.

**Command Modes** Global configuration mode

Command History	Release	Modification
	12.3(9a)BC	This command was introduced on the Cisco uBR10012 and Cisco uBR7246VXR universal broadband routers.

**Usage Guidelines** Use the **show cable logging** command to check whether the logging feature is enabled and the status of the logging buffer.

**Examples** The following example shows how to clear the log buffer that contains a bad IP source address error messages:

```
Router# show cable logging summary
Cable logging: BADIPSOURCE Enabled
Total buffer size (bytes): 1000000
Used buffer size (bytes) : 36968
Logged messages : 231
Router# clear cable logging badipsource
Router# show cable logging summary
Cable logging: BADIPSOURCE Enabled
Total buffer size (bytes): 1000000
Used buffer size (bytes) : 0
Logged messages : 0
```

Related Commands	Command	Description
	cable logging badipsource	Logs error messages about bad IP source addresses on the cable interfaces to a separate log buffer,
	show cable logging	Indicates whether the logging feature is enabled and the status of the logging buffer.

For additional information about logging events on the Cisco CMTS, refer to the following document on Cisco.com:

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

## cable source-verify

To enable verification of IP addresses or service IDs (SIDs) for CMs and CPE devices on the upstream, use the **cable source-verify** command in global configuration, cable interface configuration or subinterface configuration modes. To disable verification, use the **no** form of this command.

### Cable Interface and Subinterface Configuration Modes

```
cable source-verify [dhcp | leasetimer value | leasequery-filter upstream query-num interval]  
no cable source-verify
```

### Global Configuration Mode

```
cable source-verify leasequery-filter downstream query-num interval  
no cable source-verify
```

Syntax Description	
<b>dhcp</b>	(Optional) Specifies that queries will be sent to verify unknown source IP addresses in upstream data packets.  <b>Note</b> Do not enable the local DHCP server on the Cisco CMTS and configure local DHCP address pools, using the <b>ip dhcp pool</b> command, when using this option, because this prevents DHCP address validation.
<b>leasetimer</b> <i>value</i>	(Optional) Specifies the time, in minutes, for how often the router should check its internal CPE database for IP addresses whose lease times have expired. The valid range for value is 1 to 240 minutes, with a default of 60 minutes.  <b>Note</b> The <b>leasetimer</b> option takes effect only when the <b>dhcp</b> option is also used on an interface. Also, this option is supported only on the master interface and cannot be configured on subinterfaces. Configuring it for a master interface automatically applies it to all subinterfaces.
<b>leasequery-filter upstream</b> <i>query-num interval</i>	(Optional) Enables upstream lease queries to be defined on a per-SID basis to reduce the chance of Denial of Service attacks. <ul style="list-style-type: none"> <li>• <i>query-num</i>— Number of leased queries per SID.</li> <li>• <i>interval</i>—Size of timer window in seconds.</li> </ul>
<b>leasequery-filter downstream</b> <i>query-num interval</i>	(Optional) Enables downstream lease queries to be defined on a per-SID basis to reduce the chance of Denial of Service attacks. <ul style="list-style-type: none"> <li>• <i>query-num</i>— Number of leased queries for an unknown SID.</li> <li>• <i>interval</i>—Size of timer window in seconds.</li> </ul>

**Defaults**

Disabled. When the **dhcp** option is specified, the **leasetimer** option is set by default to 60 minutes.

**Command Modes**

Global configuration, Cable interface configuration or subinterface configuration



**Note** Configuring the **cable source-verify** command on the master interface of a bundle will configure it for all of the slave interfaces in the bundle as well.

**Command History**

Release	Modification
11.3 XA	This command was introduced.
12.0(7)T	The <b>dhcp</b> keyword was added.
12.0(10)SC, 12.1(2)EC	Support was added for these trains.
12.1(3a)EC	Subinterface support was added.
12.1(13)EC, 12.2(11)BC1	The <b>leasetimer</b> keyword was added.
12.2(15)BC1	The verification of CPE devices was changed when using the <b>dhcp</b> keyword.
12.2(15)BC2	Support for verifying CMs and CPE devices that are on a different subnet than the cable interface was enhanced to use Reverse Path Forwarding (RFP).
12.3(9a)BC	In order to protect the Cisco CMTS from denial of service attacks, Cisco IOS Release 12.3(9a)BC adds the option of using a per SID basis for deriving lease queries from CPE devices. This release also introduces a global rate limit for lease queries initiated by downstream traffic. These enhancements reduce the CPU utilization of DHCP Receive and ISR processes when the Cisco CMTS is configured with the <b>cable source-verify dhcp</b> and <b>no cable arp</b> commands.

For additional information about this and other commands, refer to the following document on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference*

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

**cable submgmt default**

To enable the Cisco CMTS Static CPE Override feature on the Cisco CMTS, use the **cable submgmt default** command in global configuration mode. This command enables field technicians to add a temporary CPE device behind the subscriber's cable modem. The temporary CPE device shares the same SID settings as the original CPE device, even though the temporary CPE device has a different MAC address. The original CPE device automatically changes from *dhcp cpe* to *static cpe* in the CMTS host routing tables, and the CPE device continues to receive service with the same SID. To disable Cisco CMTS Static CPE Override on the Cisco CMTS, use the **no** form of this command. This automatically updates the routing tables and enables the MAC address from the technician's laptop for a future field service connection at a different location.

```
cable submgmt default { active | filter-group { cm | cpe } | learnable | max-cpe }
```

```
no cable submgmt default
```

**Syntax Description**

active	Keyword enables Cisco CMTS Static CPE Override, granting local CPE control for subscriber management filtering (as defined by existing SID settings).
filter-group {cm   cpe}	<p>Keyword enables one or more temporary CPE devices to inherit the characteristics of an existing filter group, either on the downstream or the upstream of the cable modem (<b>cm</b>) or the CPE device (<b>cpe</b>).</p> <ul style="list-style-type: none"> <li><b>filter-group cm {downstream   upstream}</b>—This keyword combination enables one or more temporary CPE devices to inherit and filter by the default downstream cable modem group, or by the default upstream cable modem group.</li> <li><b>filter-group cpe {downstream   upstream}</b>—This keyword combination enables one or more temporary CPE devices to inherit and filter by the default downstream CPE group, or by the default upstream CPE group.</li> </ul>
learnable	Keyword automatically enables one or more temporary CPE devices to learn and to operate within the CPE IP address(es) in the Cisco CMTS routing table.
max-cpe	Keyword sets the maximum number of IP addresses to be permitted behind a cable modem while the Cisco CMTS Static CPE Override feature is enabled. This keyword enables multiple temporary CPE devices in the range of 0 to 1024.

**Defaults**

This command is disabled by default.

**Command Modes**

Global configuration mode

**Command History**

Release	Modification
12.3(9a)BC	This feature was introduced on Cisco uBR10012 and Cisco uBR7200 series universal broadband routers.

**Usage Guidelines**

Prior to using this command, the first (existing) DHCP CPE device maintains its DHCP dynamic MAC address behind the cable modem. The SID is assigned to this IP address.

However, by enabling Static CPE override, you gain the following states and options on two CPE devices behind the cable modem.

- The SID definition on the first CPE device is assigned a different static IP address. This enables you to change the existing (dynamic) DHCP IP address to a static IP address without first clearing the DHCP CPE host entries from the Cisco CMTS. The CPE IP state changes from **dhcp** to **static cpe**.
- This static override allows a second CPE device with a second MAC address behind the same cable modem with SID1 to be assigned same IP address as the first CPE device.



**Note**

The second CPE device changes from **dhcp cpe** to **static CPE** in the CMTS host tables.

**Examples**

The following example enables Cisco CMTS Static CPE Override in the field, enabling more or more additional CPE devices to be added behind a subscriber's cable modem:

```
Router(config)# cable submgmt default active
```

The following example configures the Cisco CMTS to accept a temporary CPE device, which inherits and filters by the subscriber's default downstream cable modem group:

```
Router(config)# cable submgmt default filter-group cm downstream
```

The following example configures the Cisco CMTS to accept a temporary CPE device, and to update the temporary CPE device with the current routing table from the Cisco CMTS:

```
Router(config)# cable submgmt default learnable
```

The following example configures the Cisco CMTS to accept a maximum of five temporary CPE devices behind a subscriber's cable modem:

```
Router(config)# cable submgmt default max-cpe 5
```

**Related Commands**

Command	Description
show cable host	Displays the CPE devices (hosts) residing behind a specified cable modem (MAC address).

**show cable tech-support**

Cisco IOS Release 12.3(9a)BC introduces changes to the output of the **show cable tech-support** command. This change allows users with large numbers of online cable modems to collect the necessary information without consuming the console session for a long period of time.

To display general information about the router when reporting a problem, use the **show cable tech-support** command in privileged EXEC mode.

```
show cable tech-support [cable slot/port | cable slot/subslot/port]
```

**Syntax Description**

<b>cable</b> slot/port	(Optional) Displays information only for the specified cable interface on the Cisco uBR7100 series and Cisco uBR7200 series routers.  On the Cisco uBR7100 series router, the only valid value is <b>1/0</b> . On the Cisco uBR7200 series router, <i>slot</i> can range from 3 to 6, and <i>port</i> can be 0 or 1, depending on the cable interface.
<b>cable</b> slot/subslot/port	(Optional) Displays information only for the specified cable interface on the Cisco uBR10012 router. The following are the valid values: <ul style="list-style-type: none"> <li>• <i>slot</i> = 5 to 8</li> <li>• <i>subslot</i> = 0 or 1</li> <li>• <i>port</i> = 0 to 4 (depending on the cable interface)</li> </ul>

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

No default behavior or values

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.1(1a)T1	This command was modified to include information about the cable clock card.
	12.2(15)BC2	This command added several <b>show pxf</b> commands to the display on the Cisco uBR10012 router.
	12.3(9a)BC	The output of the command was significantly shortened by moving a number of <b>show</b> commands (the ones that display information about individual cable modems) to the <b>show tech-support</b> command. Also, added support for an option to display information about only one specific cable interface.

**Examples**

The following example illustrates the cable modem and interface information for the Cisco uBR10012 router on which Cisco IOS Release 12.3(9a)BC is installed.

```
Router# show cable tech-support
----- Slot 8/1 -----
----- show cable modem Cable8/1/0 -----
MAC Address      IP Address      I/F      MAC          Prim RxPwr  Timing  Num BPI
                  State          Sid (dB)  Offset  CPE Enb
----- show cable modem Cable8/1/0 connectivity -----
Prim 1st time  Times %online  Online time  Offline time
Sid  online   Online      min  avg  max  min  avg  max
----- show interface Cable8/1/0 sid -----
Sid  Prim  MAC Address  IP Address  Type Age      Admin  Sched  Sfid
                  State  Type
----- show interface Cable8/1/0 sid counter -----
Sid  Req-polls  BW-reqs  Grants  Packets  Frag  Concatpkts
      issued   received  issued  received  complete  received
----- show interface Cable8/1/0 sid association -----
Sid  Prim Online   IP Address  MAC Address  Interface  VRF Name
----- show interface Cable8/1/0 modem 0 -----
SID  Priv bits  Type      State      IP address  method  MAC address
----- show cable modem Cable8/1/1 -----
MAC Address      IP Address      I/F      MAC          Prim RxPwr  Timing  Num BPI
                  State          Sid (dB)  Offset  CPE Enb
----- show cable modem Cable8/1/1 connectivity -----
Prim 1st time  Times %online  Online time  Offline time
Sid  online   Online      min  avg  max  min  avg  max
----- show interface Cable8/1/1 sid -----
Sid  Prim  MAC Address  IP Address  Type Age      Admin  Sched  Sfid
                  State  Type
----- show interface Cable8/1/1 sid counter -----
Sid  Req-polls  BW-reqs  Grants  Packets  Frag  Concatpkts
      issued   received  issued  received  complete  received
----- show interface Cable8/1/1 sid association -----
Sid  Prim Online   IP Address  MAC Address  Interface  VRF Name
----- show interface Cable8/1/1 modem 0 -----
SID  Priv bits  Type      State      IP address  method  MAC address
```

For additional information about this and other commands, refer to the following document on Cisco.com:

- *Cisco IOS CMTS Cable Command Reference*

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

## show controllers cable

Cisco IOS Release 12.3(9a)BC adds the **tech-support** keyword to the **show controllers cable** command. This change allows users with large numbers of online cable modems to collect the necessary line card information without consuming the console session for a long period of time.

Additional and related improvements are also available for the **show tech-support** command.

To display information about the interface controllers for a cable interface on the Cisco CMTS router, use the **show controllers cable** command in user EXEC or privileged EXEC mode.

```
show controllers cable { slot/port | slot/subslot/port } [downstream | upstream [port]] [mem-stat]
[memory] [proc-cpu] [tech-support]
```

Syntax	Description
<i>slot/port</i>	Identifies the cable interface and downstream port on the Cisco uBR7100 series and Cisco uBR7200 series routers.  On the Cisco uBR7100 series router, the only valid value is <b>1/0</b> . On the Cisco uBR7200 series router, <i>slot</i> can range from 3 to 6, and <i>port</i> can be 0 or 1, depending on the cable interface.
<i>slot/subslot/port</i>	Identifies the cable interface on the Cisco uBR10012 router. The following are the valid values: <ul style="list-style-type: none"> <li>• <i>slot</i> = 5 to 8</li> <li>• <i>subslot</i> = 0 or 1</li> <li>• <i>port</i> = 0 to 4 (depending on the cable interface)</li> </ul>
<b>downstream</b>	(Optional) Displays downstream interface status.
<b>upstream</b>	(Optional) Displays upstream interface status.
<i>port</i>	(Optional) Specifies the desired upstream port. Valid values start with 0 for the first upstream port on the cable interface line card.
<b>mem-stat</b>	(Optional) Displays the output from the <b>show memory statistics</b> command to display a summary of memory statistics for a Broadband Processing Engine (BPE) cable interface line card.
<b>memory</b>	(Optional) Displays the output from the <b>show memory</b> command to display a summary of memory statistics, including the memory as it is allocated per process, for a Broadband Processing Engine (BPE) cable interface line card.
<b>proc-cpu</b>	(Optional) Displays the output from the <b>show processes cpu</b> command to display the processor status for a Broadband Processing Engine (BPE) cable interface line card.
<b>tech-support</b>	(Optional, privileged EXEC mode only) Displays the output from the <b>show cable tech-support</b> command for a Broadband Processing Engine (BPE) cable interface line card.

**Command Modes** User EXEC, Privileged EXEC

**Command History**

Release	Modification
11.3 NA	This command was introduced.
12.0(2)XC	This command was modified to show a number of additional fields.
12.1(5)EC1	Support was added for the Cisco uBR7100 series router, including information about the Cisco uBR7100 series integrated upconverter.
12.2(1)XF1	Support was added for the Cisco uBR10012 router.
12.0(16)SC2, 12.1(10)EC1, 12.2(4)BC1b	The algorithm for calculating the SNR value was enhanced for a more accurate value.
12.2(15)CX	Support was added for the Cisco uBR-MC28U/X cable interface line card, including the display of the number of packets dropped because they were for a Service Flow ID (SFID) of 0.
12.2(15)BC2b	The <b>mem-stat</b> , <b>memory</b> , and <b>proc-cpu</b> options were added to obtain processor 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 uBR10-MC5X20S/U cards.
12.3(9a)BC	The <b>tech-support</b> option was added in order to improve command behavior. Additional information required during technical support is also available with alternate commands such as <b>show tech-support</b> and <b>show cable tech-support</b> .

**Usage Guidelines**

The **mem-stat**, **memory**, and **proc-cpu** keywords execute the related command on the processor that runs on 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 uBR10-MC5X20S/U cards. This allows you to obtain information that is specific for that particular cable interface card, as opposed to having to run these commands on the entire router.



**Note** The **mem-stat**, **memory**, and **proc-cpu** options are not available for cable interface line cards that do not contain an onboard processor (for example, the Cisco uBR-MC16C cable interface line card).

**Examples**

The following is sample output for the downstream connection for cable interface 8/1/0 on a Cisco uBR10012 router:

```
Router# show controllers c8/1/0 downstream
Cable8/1/0 Downstream is up
Frequency not set, Channel Width 6 MHz, 64-QAM, Symbol Rate 5.056941 Msps
FEC ITU-T J.83 Annex B, R/S Interleave I=32, J=4
Downstream channel ID: 0
Dynamic Services Stats:
DSA: 0 REQs 0 RSPs 0 ACKs
0 Successful DSAs 0 DSA Failures
DSC: 0 REQs 0 RSPs 0 ACKs
0 Successful DSCs 0 DSC Failures
DSD: 0 REQs 0 RSPs
0 Successful DSDs 0 DSD Failures
DCC: 0 REQs 0 RSPs 0 ACKs
0 Successful DCCs 0 DCC Failures
```

Table 16 describes the fields displayed by the **show controllers cable downstream** command.

**Table 16** *show controllers cable downstream Field Descriptions*

Field	Description
Cable	Slot number/port number indicating the location of the Cisco cable interface line card.
Downstream is up	Indicates that the RF downstream interface is enabled.
Frequency	Transmission frequency of the RF downstream. (This information may not match the current transmission frequency, which is external on CMTS platforms that use an external upconverter.)
Channel Width	Indicates the width of the RF downstream channel.
QAM	Indicates the modulation scheme.
Symbol Rate	Indicates the transmission rate (in number of symbols per second).
FEC ITU-T	Indicates the Motion Picture Experts Group (MPEG) framing standard.
R/S Interleave I/J	Indicates Reed Solomon framing based on ITU S.83-B.

## Examples

The following example illustrates the information from the **show controllers cable** command for slot/subslot/port 8/1/0 on a Cisco uBR10012 router on which Cisco IOS Release 12.3(9a)BC is installed.

```
Router# show controllers c8/1/0
Interface Cable8/1/0
Hardware is MC28C(F-connector)
BCM3210 revision=0x56B2
idb 0x61329EB0 MAC regs 0x3E104000 PLX regs 0x3E000000
rx ring entries 1024 tx ring entries 128 MAP tx ring entries 128
Rx ring 0xC1AD080 shadow 0x613AAB38 head 0
Tx ring 0xC1AF0C0 shadow 0x613ABBA8 head 34 tail 34 count 0
MAP Tx ring 0xC1AF500 shadow 0x613AC018 head 52 tail 52 count 0
Timestamp is from TCCplus card
throttled 0 enabled 0 disabled 0
Rx: spurious 0 framing_err 0 hcs_err 0 no_buffer 0 short_pkt 0
    no_enqueue 0 no_enp 0 miss_count 0 latency 0
    invalid_sid 0 invalid_mac 0 bad_ext_hdr_pdu 0 concat 0 bad-concat 0
Tx: full 0 drop 0 stuck 0 latency 20
MTx: full 0 drop 0 stuck 0 latency 10
Slots 0 NoUWCollNoEngy 0 FECorHCS 1 HCS 1
Req 3842362657 ReqColl 0 ReqNoise 0 ReqNoEnergy 3842362657
ReqData 32 ReqDataColl 0 ReqDataNoise 0 ReqDataNoEnergy 32
Rng 0 RngColl 0 RngNoise 0
FECBlks 1 UnCorFECBlks 1 CorFECBlks 0
MAP FIFO overflow 0, Rx FIFO overflow 0, No rx buf 0
DS FIFO overflow 0, US FIFO overflow 0, US stuck 0
Bandwidth Requests= 0x0
--More--
```

The following example illustrates memory statistics for the specified slot/subslot/port on the Cisco uBR10012 router:

```
Router# show controllers c8/1/0 mem-stat
          Head    Total(b)    Used(b)    Free(b)    Lowest(b)    Largest(b)
Processor 60F3FB40 185337024  8644376   176692648 176557288   176638828
          I/O    C000000    67108864  6679384   60429480   60429480   60405696
```

The following example illustrates upstream information for the specified slot/subslot/port on the Cisco uBR10012 router:

```
Router# show controllers c8/1/0 upstream
Cable8/1/0 Upstream 0 is up
  Frequency 25.008 MHz, Channel Width 1.600 MHz, QPSK Symbol Rate 1.280 Msps
  Spectrum Group is overridden
  SNR - Unknown - no modems online.
  Nominal Input Power Level 0 dBmV, Tx Timing Offset 0
  Ranging Backoff automatic (Start 0, End 3)
  Ranging Insertion Interval automatic (60 ms)
  Tx Backoff Start 3, Tx Backoff End 5
  Modulation Profile Group 1
  Concatenation is enabled
  Fragmentation is enabled
  part_id=0x3137, rev_id=0x03, rev2_id=0xFF
  nb_agc_thr=0x0000, nb_agc_nom=0x0000
  Range Load Reg Size=0x58
  Request Load Reg Size=0x0E
  Minislot Size in number of Timebase Ticks is = 4
  Minislot Size in Symbols = 32
  Bandwidth Requests = 0x0
  Piggyback Requests = 0x0
  Invalid BW Requests= 0x0
  Minislots Requested= 0x0
  Minislots Granted = 0x0
  Minislot Size in Bytes = 8
  Map Advance (Dynamic) : 2180 usecs
  UCD Count = 320676
  DES Ctrl Reg#0 = C000C043, Reg#1 = 0
```

The following example illustrates CPU processes for the specified slot/subslot/port on the Cisco uBR10012 router:

```
Router# show controllers c8/1/0 proc-cpu
CPU utilization for five seconds: 1%/1%; one minute: 1%; five minutes: 1%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
  1         4           1          4000   0.00%  0.00%  0.00%  0 Chunk Manager
  2         0        128036           0   0.00%  0.00%  0.00%  0 Load Meter
  3        248          395          627   0.00%  0.00%  0.00%  0 CR10K IPC MSG Pr
  4       428012     384113         1114   0.07%  0.07%  0.07%  0 CR10K NonBlk Xmt
  5       43392     65009          667   0.00%  0.00%  0.00%  0 Check heaps
  6         8           561          14   0.00%  0.00%  0.00%  0 Pool Manager
  7         0           1           0   0.00%  0.00%  0.00%  0 AAA_SERVER_DEADT
  8         0           2           0   0.00%  0.00%  0.00%  0 Timers
  9         0           2           0   0.00%  0.00%  0.00%  0 AAA high-capacit
 10         0        10680           0   0.00%  0.00%  0.00%  0 ARP Input
 11         0           1           0   0.00%  0.00%  0.00%  0 Entity MIB API
 12         0           2           0   0.00%  0.00%  0.00%  0 Serial Backgroun
```

The following example illustrates memory processor information for the specified slot/subslot/port on the Cisco uBR10012 router:

```
Router# show controllers c8/1/0 memory
          Head      Total(b)      Used(b)      Free(b)      Lowest(b)      Largest(b)
Processor 60F3FB40 185337024 8644376 176692648 176557288 176638828
          I/O      C000000 67108864 6679384 60429480 60429480 60405696
Processor memory
Address   Bytes      Prev      Next Ref      PrevF      NextF Alloc PC what
60F3FB40 0000020004 00000000 60F4498C 001 ----- ----- 60113308 Managed Chunk Queue
Elements
60F4498C 0000001504 60F3FB40 60F44F94 001 ----- ----- 60126F88 List Elements
60F44F94 0000005004 60F4498C 60F46348 001 ----- ----- 60126FCC List Headers
60F46348 0000000048 60F44F94 60F463A0 001 ----- ----- 6055D4E4 *Init*
60F463A0 0000000028 60F46348 60F463E4 001 ----- ----- 604C12B4 *Init*
60F463E4 0000000048 60F463A0 60F4643C 001 ----- ----- 6055D4E4 *Init*
```

```
60F4643C 0000000200 60F463E4 60F4652C 001  ----- 6014BE28 *Init*
60F4652C 0000004260 60F4643C 60F475F8 001  ----- 60065A2C TTY data
60F475F8 0000002004 60F4652C 60F47DF4 001  ----- 60069164 TTY Input Buf
```

The following example illustrates the first information for the **tech-support** option for the specified slot/subslot/port on the Cisco uBR10012 router:

```
Router# show controllers c8/1/0 tech-support
----- show version -----
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (UBR10KCLC-LC-M), Experimental Version 12.3(20040708:1441
55) [bguckel-geo_cable-l2 102]
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Mon 12-Jul-04 11:28 by bguckel
Image text-base: 0x60008EB8, data-base: 0x60CB0000
ROM: System Bootstrap, Version 12.2(20011031:221132) [maheshj-cr10k-rommon 15],
DEVELOPMENT SOFTWARE
BOOTLDR: 7200 Software (UBR10KCLC-LC-M), Experimental Version 12.2(20011107:2331
03) [janez-v122_2_xf_throttle.Nov5A 101]
clc_8_1 uptime is 1 week, 9 hours, 54 minutes
System returned to ROM by power-on
System restarted at 08:59:44 UTC Wed Jul 21 2004
Running default software
cisco uBR10K CLC (NPE-CLC) processor (revision A) with 196608K/65536K bytes of m
emory.
Processor board ID
R7000 CPU at 262MHz, Implementation 39, Rev 2.1, 256KB L2 Cache
6 slot midplane, Version 1.0
For additional information about this and other commands, refer to the following document on
Cisco.com:

```

- *Cisco IOS CMTS Cable Command Reference*

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

## show tech-support

Cisco IOS Release 12.3(9a)BC shortens the output of the **show tech-support** command on the Cisco uBR10012 and the Cisco uBR7246VXR routers. This change allows users with large numbers of online cable modems to collect information without consuming the console session for a long period of time.

To display general information about the Cisco CMTS router when reporting a problem to Cisco technical support, use the **show tech-support** command in privileged EXEC mode.

```
show tech-support [page] [password] [cef | ipc | ipmulticast | isis | mpls | ospf | rsvp]
```



**Note**The **show tech-support** command automatically displays the output of a number of different **show** commands. The exact output depends on the platform, configuration, and type of protocols being used.



**Note**The **show tech-support** includes most of the information shown in the **show cable tech-support** command.

Syntax Description	
<b>page</b>	(Optional) Causes the output to display a page of information at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, does not stop for page breaks).
<b>password</b>	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label “<removed>” (this is the default).
<b>cef</b>	(Optional) Displays information about the Cisco Express Forwarding (CEF) protocol configuration and status.
<b>ipc</b>	(Optional) Displays information about interprocess communications on the Cisco router.
<b>ipmulticast</b>	(Optional) Displays information about the IP multicast configuration and status.
<b>isis</b>	(Optional) Displays information about the Connectionless Network Service (CLNS) and Intermediate System-to-Intermediate System (IS-IS) routing protocol configuration and status.  <b>Note</b> IS-IS support is provided only on CMTS platforms running Cisco IOS images that have a “-p-” as part of the image name.
<b>mpls</b>	(Optional) Displays information about Multiprotocol Label Switching (MPLS) on the Cisco router, which instructs the routers and the switches in the network on where to forward the packets based on preestablished IP routing information.  <b>Note</b> Cisco IOS Release with the Cisco uBR10012 router does not support overlapping IP addresses with MPLS Virtual Private Networks (VPN).
<b>ospf</b>	(Optional) Displays information about the Open Shortest Path First (OSPF) routing algorithm and status on the Cisco router.
<b>rsvp</b>	(Optional) Displays information about the IP Resource Reservation Protocol (RSVP) configuration and status.

For additional information about this and other commands, refer to the following document on Cisco.com (updated through Cisco IOS Release 12.3(9a)BC):

- *Cisco IOS CMTS Cable Command Reference*

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

# Caveats for Cisco IOS Release 12.3 BC

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.

Cisco IOS Release 12.3 mainline is the parent release train for 12.3(23)BC7. Unless otherwise noted, Cisco IOS Release 12.3(23)BC7 maintains support for the changes and caveat resolutions introduced in earlier releases of Cisco IOS Release 12.3 mainline.



**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 <http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>

## Open Caveats for Release 12.3(23)BC10

Table 17 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(23)BC10.

**Table 17** Open Caveats for Cisco IOS Release 12.3(23)BC10

DDTS ID Number	Description
CSCeh33888	<p>Symptoms: A Cisco uBR7246VXR router may reload with the configurations set during the last watchdog reset.</p> <p>Conditions: This issue occurs on a Cisco uBR7246VXR router having a Cisco uBR7200-NPE-G1 processor board, and running Cisco IOS Release 12.3(9a)BC.</p> <p>Workaround: There is no workaround.</p>
CSCs150133	<p>Symptoms: The Cisco uBR7246VXR router reloads with the following message:</p> <pre>No crashinfo No tracebacks Last reload reason: Unknown reason Last reset from watchdog reset</pre> <p>Conditions: This issue occurs on a Cisco uBR7246VXR router with UBR7200-NPE-G1, running Cisco IOS Release 12.3(17b)BC4.</p> <p>Workaround: There is no workaround.</p>
CSCsz98503	<p>Symptoms: There is a time delay of a few minutes when multiple cable modems go off on a random upstream. These losses are usually accompanied by a spike in the error per second rate or by an MER drop and a decrease in docsIfSigQUnerrored MIB. However, the reverse is not true—a brief degradation of the physical connectivity parameters does not necessarily trigger a brief CM loss.</p> <p>Conditions: This issue occurs on the Cisco uBR10-MC5X20H line cards.</p> <p>Workaround: There is no workaround.</p>

**Table 17**      **Open Caveats for Cisco IOS Release 12.3(23)BC10 (continued)**

DDTS ID Number	Description
CSCtc49858	<p>Symptoms: Users with lower privilege levels than "Enable access" may not be able to execute some "show cable" command options, since they do not carry over the right privilege level as their parent.</p> <p>For example, in Enabled mode:</p> <pre>UBR10K-1#show cable mac-domain Cable6/0/4 ?   cgd-associations          CGD Downstream Association   downstream-service-group  MAC Domain service groups &lt;==== Available                              under Enable mode.</pre> <p>Now, when you assign this command to user mode with a different privilege level:</p> <pre>  privilege exec level 1 show cable mac-domain</pre> <p>Not all command options under the <b>show cable mac-domain</b> parent command are available. In this example, the downstream-service-group option is not available:</p> <pre>UBR10K-1#enable 1 UBR10K-1&gt;show cable mac-domain Cable6/0/4 ?   cgd-associations          CGD Downstream Association UBR10K-1&gt;show cable mac-domain Cable6/0/4 downstream-service-group                                      ^ % Invalid input detected at '^' marker.</pre> <p>But, the other option is available:</p> <pre>UBR10K-1&gt;show cable mac-domain c6/0/4 cgd-associations Load for five secs: 4%/1%; one minute: 3%; five minutes: 2% Time source is NTP, 13:00:09.089 EDT Mon Oct 12 2009 CGD Host Resource DS Channels          Upstreams (AllUS)  Active Remote DS</pre> <p>This is not the correct behavior for privilege level command, as it should grant the same privilege for all command options configurable for the defined command.</p> <p>Conditions: This issue occurs with the <b>show cable mac-domain</b> command and its "downstream-service-group" option that displays DS channel information for Wideband cable modems. All the Cisco IOS releases 12.3BC, 12.2(33)SCB, and 12.2(33)SCC are affected.</p> <p>Workaround: Repeat the privilege level command in a more granular way.</p> <p>For example, for the example explained above, the command needs to be repeated for each interface as follows:</p> <pre>privilege exec level 1 show cable mac-domain c5/0/0 downstream-service-group privilege exec level 1 show cable mac-domain c5/0/1 downstream-service-group privilege exec level 1 show cable mac-domain c5/0/2 downstream-service-group ... ... privilege exec level 1 show cable mac-domain c8/1/4 downstream-service-group</pre>

**Table 17** *Open Caveats for Cisco IOS Release 12.3(23)BC10 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCtc78090	<p>Symptoms: The downstream frequency override (DFO) retry counter is not incremented from #0.</p> <p>Conditions: This issue occurs while configuring "cable service attribute ds-bonded downstream-type bonding-enabled [enforce]". After the wideband cable modem goes online(NB) with "ds-bonded downstream-type bonding-enabled enforce", power on and off the wideband cable modem. The DFO retry counter should be incremented after this but this does not occur.</p> <p>Workaround: There is no workaround.</p>
CSCth01285	<p>Symptoms: Multicast traffic is not forwarded across DOCSIS Set-Top Gateway (DSG) tunnels on modular and legacy downstreams.</p> <p>Conditions: This issue is observed on Cisco uBR10012 router.</p> <p>Workaround: Re-configure the DSG tunnels.</p>

## Resolved Caveats for Release 12.3(23)BC10

Table 18 lists only severity 1 and 2 caveats and select severity 3 resolved caveats for Cisco IOS Release 12.3(23)BC10.

**Table 18** *Resolved Caveats for Cisco IOS Release 12.3(23)BC10*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsz45567	<p>A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).</p> <p>A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process. A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).</p> <p>Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.</p> <p>This advisory is posted at:  <a href="http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml</a></p>
CSCsz53710	<p>Symptoms: Cannot ping or provision a Multimedia Terminal Adaptor (MTA) that has no IP connectivity.</p> <p>Conditions: This issue occurs while upgrading to Cisco IOS Release 12.2(33)SCB2.</p> <p>Workaround: Reset the MTA.</p>

**Table 18**      **Resolved Caveats for Cisco IOS Release 12.3(23)BC10 (continued)**

DDTS ID Number	Description
CSCsz75186	<p>Cisco IOS Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang. The vulnerability may be triggered by a TCP segment containing crafted TCP options that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>This advisory is posted at <a href="http://www.cisco.com/warp/public/707/cisco-sa-20100324-tcp.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20100324-tcp.shtml</a></p>
CSCtc44253	<p>Symptoms: The accumulated timing offset of a modem goes to a negative value. The following error message is displayed on the CMTS:</p> <p>"%UBR10000-4-BADTXOFFSET: Bad timing offset -182443 detected for cable modem 000a.73cc.c7b7. "</p> <p>Conditions: This issue occurs on the Cisco uBR10-MC5X20 line card.</p> <p>Workaround: There is no workaround.</p>
CSCtc07585	<p>Symptoms: The standby PRE crashes during the cable modem entry cleanup.</p> <p>Conditions: This issue is seen on the Cisco uBR10012 (PRE 2) running the Cisco IOS Release 12.2(33)SCB4. This issue is seen when there are many cable modems and service flows on the network and there is congestion between the active and standby Router Processors, which could lead to the IPC packet drop.</p> <p>Workaround: There is no workaround.</p>
CSCtc19290	<p>Symptoms: PRE crashes after OIR or crash of the cable line card.</p> <p>Conditions: This issue occurs when a bundle member cable line card is removed from the system before it is removed from the running configuration. This crashes the active PRE and the cable line card. This problem does not occur with every OIR, however, it occurs when there is a punted packet associated with the OIR/crashed interface.</p> <p>Workaround: Remove the cable line card from the bundle configuration (running config) before OIR of the card.</p>
CSCtf48376	<p>Symptoms: A crash occurs on a Cisco uBR10012 router running Cisco IOS Release 12.2(33)SCB5 with PRE-4.</p> <p>Conditions: This issue occurs when the show cable modem ip service flow verbose command is executed several times.</p> <p>Workaround: Delete the fiber node configuration and reconfigure it.</p>

**Table 18** *Resolved Caveats for Cisco IOS Release 12.3(23)BC10 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCti25339	<p>Symptoms: Cisco IOS device may experience a device reload.</p> <p>Conditions: This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.</p> <p>Workaround: There is no workaround.</p> <p>PSIRT Evaluation:</p> <p>The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:  <a href="https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&amp;version=2&amp;vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C">https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&amp;version=2&amp;vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C</a></p> <p>CVE ID CVE-2010-3050 has been assigned to document this issue.</p> <p>Additional information on Cisco's security vulnerability policy can be found at the following URL:  <a href="http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html">http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html</a></p>
CSCti81896	<p>Symptoms: When the ingress cancellation feature is enabled, all modems on an upstream may momentarily go offline and then recover within minutes. This problem is not observed when the ingress cancellation feature is disabled.</p> <p>Conditions: This issue occurs because the Rogue modems may transmit during ingress cancellation idle period. During this period, modems should not transmit. One or more modems consistently transmitting at this time period can create poor ingress cancellation performance for the burst receiver, and in the worst case situation, it can cause all modems to go offline momentarily until the upstream receiver re-adapts.</p> <p>Workaround: Disable the ingress cancellation feature for that upstream, for which the rogue modems failures are encountered.</p>

**Table 18 Resolved Caveats for Cisco IOS Release 12.3(23)BC10 (continued)**

DDTS ID Number	Description
CSCtk09023	<p>Symptoms: The service flow ID does not appear under scm service-flow main but appears under service-flow detail.</p> <p>Conditions: This issue occurs with Cisco IOS Release 12.3(23)BCx, Cisco IOS Release 12.2(33)SCBx, Cisco IOS Release 12.2(33)SCCx and Cisco IOS Release 12.2(33)SCDx. The Cisco uBR10012 router may have service flow mismatch between the route processor and the cable line card when there is a high CPU usage by the line card or when there is a huge traffic load on the IPC bus due to mass cable modem registration events like an RF node failure. This affects both the upstream and downstream secondary service flows that are local or remote. When the downstream is remote, the CMTS reports 0 blaze index error for the affected downstream service flow.</p> <p>For example,</p> <pre>scm 0011.e6fe.55ce service-flow Sfid Dir Curr Sid Sched Prio MaxSusRate MaxBrst MinRsvRate Throughput       State      Type 26429 US act 5290 BE 1 1024000 10000000 0 68 26441 US act 5296 NRTPS 4 64000 3044 32000 0 &lt;-- Here 26430 DS act N/A BE 1 6600000 12000000 0 0 26442 DS act N/A BE 4 64000 96000 32000 0  UPSTREAM SERVICE FLOW DETAIL: SFID SID Requests Polls Grants Delayed Dropped Packets       Grants Grants 26429 5290 86 0 86 0 0 30 26439 5290 86 0 86 0 0 30 &lt;-- Here</pre> <p>Workaround: There is no workaround.</p>
CSCtl79450	<p>Symptoms: High CPU usage during SNMP polling using OID docsQosMacToSrvFlowTable.</p> <p>Conditions: This issue occurs during SNMP query on the docsQosMacToSrvFlowTable when the cable interfaces are located at the end of the list resulting in a search loop.</p> <p>Workaround: Stop querying this table.</p>

## Open Caveats for Release 12.3(23)BC9

Table 19 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(23)BC9.

**Table 19** Open Caveats for Cisco IOS Release 12.3(23)BC9

DDTS ID Number	Description
CSCsv63445	<p>Symptoms: The <b>clear cable modem</b> command does not reset the modular-host tables.</p> <p>Conditions: This issue occurs in the following conditions when you have:</p> <ul style="list-style-type: none"> <li>not configured any fiber nodes.</li> <li>brought some narrow-band modems online from the SPA downstream.</li> <li>used the <b>clear cable modem all reset</b> command to reset the modems.</li> </ul> <p>After execute the <b>clear cable modem all reset</b> command, all the statistics, baseline privacy interface (BPI), and payload header suppression (PHS) indexes in the modular-host tables are expected to be freed, but are not freed.</p> <p>This causes a leak in the statistics, baseline privacy interface (BPI), and payload header suppression (PHS) indexes and raises a Cable Modem Transmission System (CMTS) scalability issue, that is, CMTS is unable to support the stated number of modems online from the SPA downstream.</p> <p>Workaround: There is no workaround.</p>
CSCsz22219	<p>Symptoms: The Cisco uBR10000 series universal broadband router with PRE2 running Cisco IOS Releases 12.3(23)BC, Cisco IOS Releases 12.3(21a)BC, or Cisco IOS Releases 12.2(33)SCB crashes.</p> <p>Conditions: This issue occurs when the PRE2 is running either Cisco IOS Releases 12.3(23)BC, Cisco IOS Releases 12.3(21a)BC, or Cisco IOS Releases 12.2(33)SCB, enabling ESR-HH-1GE. The <b>cable source-verify dhcp</b> command is executed but no cable line card is configured or inserted.</p> <p>Workaround: Configure or insert the cable line card in the Cisco CMTS.</p>
CSCsz49382	<p>Symptoms: Cable modems do not respond to Layer 3 pings.</p> <p>Conditions: This issue occurs only on the Cisco uBR10-MC5X20S and Cisco uBR10-MC5X20U line cards when PRE-EQ (equalization-coefficient) is configured.</p> <p>Workaround: Reset the cable line card.</p>
CSCsz98503	<p>Symptoms: There may be sporadic short losses (of a few minutes) of multiple CMs off a (random) upstream. These losses are usually accompanied by a spike of error per second rate or drop in modulation error ratio (MER) and a decrease in the <b>docsIfSigQUnerrored</b>s.</p> <p>However, the reverse is not true—a brief degradation of the physical connectivity parameters does not necessarily trigger a brief CM loss.</p> <p>Conditions: This issue occurs on Cisco uBR10-MC5X20H line cards.</p> <p>Workaround: There is no workaround.</p>

**Table 19**      **Open Caveats for Cisco IOS Release 12.3(23)BC9 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCta32429	<p>Symptoms: Non-bonding cable modems are wrongly registered in bonded channels.</p> <p>Workaround: There is no workaround.</p>
CSCta38298	<p>Symptoms: Active PRE fails over to the secondary reporting.</p> <p>Conditions: This issue is observed in Cisco IOS Release 12.3(23)BC7.</p> <p>Workaround: There is no workaround.</p>
CSCtb93407	<p>Symptoms: The system logs record a line-card crash (8/0), which is immediately followed by a PRE failover.</p> <p>Conditions: There is no query on the MIB object, <b>cefcFRUPowerSupply-GroupTable</b>, when the failover occurs.</p> <p>Workaround: There is no workaround.</p>
CSCtc39722	<p>Symptoms: Modems do not come online, or once online quickly return to the offline state, on interfaces with modular remote primary.</p> <p>The <b>show cable modem primary summary total</b> command displays the non-zero blaze indices stay non-zero:</p> <p>Conditions: This issue occurs on a PRE failover event and when modems are on a domain that has only modular remote primaries.</p> <p>This issue is observed on Cisco uBR10000 with PRE2 running Cisco IOS Release 12.3(23)BC7.</p> <p>Workaround: Power cycle the affected line card.</p>
CSCtc49858	<p>Symptoms: If you have lower privilege levels than Enable Access, you may not be able to execute some <b>show cable</b> command options.</p> <p>Conditions: This issue occurs because the parent privilege level is not carried over correctly. This issue is observed on the Cisco CMTS with the Cisco IOS Release 12.3BC, Cisco IOS Release 12.2SCB, and Cisco IOS Release 12.2SCC.</p> <p>Workaround: Repeat the privilege level command for each interface.</p>
CSCtc59089	<p>Symptoms: The cable line card (CLC) crashes when a specific 3-way call scenario is initiated.</p> <p>Conditions: This issue occurs where multiline AT attachments (ATAs) are placed behind CMs in a PCMM setup.</p> <p>Workaround: There is no workaround.</p>
CSCtc78090	<p>Symptoms: The downstream frequency override (DFO) retry counter does not rise beyond the number zero.</p> <p>Conditions: This issue occurs when you execute the <b>cable service attribute ds-bonded downstream-type bonding-enabled [enforce]</b> command and then power on and off the wideband cable modem.</p> <p>Workaround: There is no workaround.</p>

**Table 19** *Open Caveats for Cisco IOS Release 12.3(23)BC9 (continued)*

DDTS ID Number	Description
CSCtc78143	Symptoms: The standby PRE crashes with a value of signal 10 after a spurious memory access. The crash only affects redundancy and has no impact on services. Workaround: There is no workaround.
CSCtc99509	Symptoms: Cisco Wideband SPA sends only "sync Tx" packets. Conditions: This issue is observed after Cisco Wideband SPA reloads and when a DOCSIS timing interface (DTI) server is used. Workaround: Reload the jacket card, reload Edge Quadrature Amplitude Modulation (EQAM), and reboot.

## Resolved Caveats for Release 12.3(23)BC9

Table 20 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(33)BC9.

**Table 20** *Resolved Caveats for Cisco IOS Release 12.3(23)BC9*

DDTS ID Number	Description
CSCek76084	Symptoms: A packetcable validate type length value (TLV) traceback occurs after a release complete (RLC) upgrade. Conditions: This issue is caused by an invalid service flow (NULL pointer). It occurs when a Dynamic Service Change (DSC) request is made. The DSC fetches the service flow from the service flow ID (SFID) and accesses it without checking whether the pointer is NULL.
CSCsg67817	Symptoms: Malformed H.245 packets crashes the IOS-based H.323 gateway. Conditions: This issue occurs when the H.323 gateway is configured. Workaround: There is no workaround.
CSCsj22874	Symptoms: The interprocess communication (IPC) connection between two line cards does not function correctly, which causes load-balance data synchronize information loss or HCCP synchronization loss. This issue also affects the Blaze index assignment if the Guardian line card is one of the affected line cards. Conditions: This issue occurs when there are three or more Cisco 520 line cards in a router. This issue occurs during system bootup or if three or more line cards have crashed or have reset at the same time. Workaround: If a service (Guardian, load-balance, or HCCP) or card is affected, reset the affected line cards.
CSCsk20999	Symptoms: In the object type syntax, <b>ifStackEntry</b> , the cable bundle interface is displayed as <b>ifStackHigherLayer</b> for modular downstream interfaces. Conditions: This issue occurs when the <b>ifStackEntry</b> MIB object is queried using SNMP.

Table 20 Resolved Caveats for Cisco IOS Release 12.3(23)BC9 (continued)

DDTS ID Number	Description
CSCsk78448	<p>Symptoms: An error message is displayed when the <b>show pxf cpu stati drop &lt;interface&gt;</b> command is executed when the interface is not supported by toasters, such as Ethernet, FastEthernet, and so on.</p> <p>Conditions: This issue occurs while executing the <b>show pxf cpu stati drop</b> command on interfaces, such as Ethernet, FastEthernet, and so on.</p> <p>Workaround: There is no workaround.</p>
CSCsw14622	<p>Symptoms: For deleted service flows, the last character in the "Service Class Name" field is dropped from the Subscriber Account Management Interface Specification (SAMIS) records and the SNMP MIB object <b>docsQosServiceFlow-LogServiceClassName</b>.</p> <p>Conditions: This issue is seen when the dynamic service flows associated with PCMM calls are deleted. The last character is missing from the service class name in the MIB object "docsQosServiceFlowLogServiceClassName" and SAMIS records</p> <p>Workaround: There is no workaround.</p>
CSCsw51992	<p>Symptoms: Invalid or corrupt values seen for OctetsPassed and PacketsPassed fields in the SAMIS records.</p> <p>Conditions: This issue occurs in the Cisco CMTS with Wideband SPA configured while querying the service flow counters using SAMIS, SNMP, or executing the <b>show</b> commands.</p> <p>Workaround: There is no workaround.</p>
CSCsx19200	<p>Symptoms: A cable line card (CLC) crashes when one of its upstreams is shut down.</p> <p>Conditions: This issue occurs only if the upstream route and its associated downstream are configured in load-balance groups.</p> <p>Workaround: There is no workaround.</p>
CSCsx63989	<p>Symptoms: The output "sid" is incorrect in the <b>show cable modem x.x.x.x service-flow [verbose]</b> command.</p> <p>Conditions: This issue occurs in the Cisco IOS Release 12.3(23)BC and Cisco IOS Release 12.2(33)SCB.</p> <p>Workaround: There is no workaround.</p>
CSCsx70889	<p>Symptoms: Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.</p> <p>Workaround: Cisco has released free software updates that address this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels</a></p>

**Table 20 Resolved Caveats for Cisco IOS Release 12.3(23)BC9 (continued)**

DDTS ID Number	Description
CSCsx94352	<p>Symptoms: The wideband cable interface is not able to pass traffic.</p> <p>Conditions: This issue occurs because the bonded channel to RF channel mapping configuration is missing from the SPA.</p> <p>Workaround: There is no workaround.</p>
CSCsy55647	<p>Symptoms: The ESR-PRE2 processor module crashes and the crash information logs display the following:</p> <pre data-bbox="613 562 1528 688">%UBR10K-6-US_SFID_INCONSISTENCY: US-SF found: SFID xxxx, type 0, sid 0 (yyyy), MAC aaaa.aaaa.aaaa (bbbb.bbbb.bbbb), prim_sid xxx(yyy)CMD: 'no cable service attribute voice-enabled downstream-type HA-capable'</pre> <p>Conditions: This issue occurs in Cisco IOS Release 12.3(23)BC4.</p> <p>Workaround: There is no workaround.</p>
CSCsy55849	<p>Symptoms: The <b>show controller modular-cable</b> command output displays invalid voltage measurement readings.</p> <p>Conditions: This issue occurs on the 24 RF channel SPA.</p> <p>Workaround: Re-execute the <b>show controller modular-cable</b> command.</p>
CSCsy66170	<p>Symptoms: After a PRE switchover, the wideband interfaces status on SPA drop offline. The wideband modems on these wideband interfaces also drop offline.</p> <p>Conditions: This issue occurs when the primary PRE and secondary PRE boot up at same time.</p> <p>Workaround: Boot up the secondary PRE much later than the primary PRE, or boot up the secondary PRE when the primary PRE is already up and running.</p>
CSCsz38104	<p>Symptoms: The H.323 implementation in Cisco IOS software contains a vulnerability that can be exploited remotely to cause a device running Cisco IOS software to reload.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Workaround: There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-h323">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-h323</a></p>
CSCsz56059	<p>Symptoms: The <b>cable dynamic-secret lock</b> command does not lock the rogue modem to a 10 Kbps upstream or downstream profile. The <b>show cable modem &lt;mac of rogue modem&gt; qos</b> command reports 0/0 Kbps for upstream and downstream rates for the same modem after the modem reboots or resets.</p> <p>Conditions: This issue occurs on the Cisco uBR10012 series universal broadband router with PRE2 processor module running the Cisco IOS Release 12.3(23)BC4 with <b>cable dynamic-secret lock</b> command configured under the cable interface.</p> <p>Workaround: There is no workaround.</p>

Table 20 Resolved Caveats for Cisco IOS Release 12.3(23)BC9 (continued)

DDTS ID Number	Description
CSCsz60401	<p>Symptoms: The following SPA bus error and Jacket watchdog reset are displayed on a Cisco Wideband SIP crash information log:</p> <pre>SPI FPGA: TIB SPA1 Bus Error [1/16] Machine Check Error, can be ECC or Watchdog.. ECC 1 bit errors since last time we cleared = 0 ECC 1 bit errors while up (total) = 0</pre> <p>Conditions: This issue occurs when the Cisco Wideband SPA power is shutdown and the power management hardware watches power supply violation to protect components on the SPA.</p> <p>Workaround: There is no workaround.</p>
CSCsz92784	<p>Symptoms: The IP detail record (IPDR) export records do not display an increment in the downstream counters for some cable modems. However, the upstream counters are reported correctly by the IPDR.</p> <p>Conditions: This issue occurs in routers running Cisco IOS Release 12.3(23)BC4 and Cisco IOS Release 12.3(21)BC.</p> <p>Workaround: Reset the cable modem or use SNMP poll to retrieve downstream and upstream data for a cable modem.</p>
CSCta03695	<p>Symptoms: Packetcable gates are found stuck in the ALLOC state after hardware module reset.</p> <p>Workaround: There is no workaround.</p>
CSCta18179	<p>Symptoms: A spurious memory access occurs or the Cisco CMTS crashes.</p> <p>Conditions: This issue is observed when the DOCSIS Set-Top Gateway (DSG) is configured and the line card is in protect mode.</p> <p>Workaround: Do not update the DSG configuration when protect mode is active.</p>
CSCta20709	<p>Symptoms: Traceback of "Link queue not free" occurs when the quadrature amplitude modulation (QAM) channel is removed from the wideband (WB) and modular cable (MC) interface or if the WB or MC interface is down.</p> <p>Conditions: This issue occurs on the Cisco uBR10000 series universal broadband routers when:</p> <ul style="list-style-type: none"> <li>• Dynamic bandwidth sharing (DBS) is configured.</li> <li>• QAM channel is removed or if interface is down.</li> </ul> <p>Workaround: There is no workaround.</p>
CSCta37455	<p>Symptoms: Multicast packets are punted from Parallel eXpress Forwarding (PXF) after a line card is inserted in the chassis.</p> <p>Conditions: This issue occurs on the Cisco uBR10000 series universal broadband router with PXF configured.</p> <p>Workaround: Configure the Cisco uBR10000 series universal broadband router with the <b>no ip multicast-routing</b>, command followed by the <b>ip multicast-routing</b> command.</p>

**Table 20 Resolved Caveats for Cisco IOS Release 12.3(23)BC9 (continued)**

DDTS ID Number	Description
CSCta37907	<p>Symptoms: The system is unable to unconfigure the cable metering during the IPDR process.</p> <p>Workaround: There is no workaround.</p>
CSCta42189	<p>Symptoms: The Wideband SPA in Cisco SIP-600 is found stuck after executing the <b>hardware-module bay x/y shutdown</b> and <b>no shutdown</b> commands.</p> <p>Workaround: Reload the Wideband SPA.</p>
CSCta42483	<p>Symptoms: Tracebacks appear while unconfiguring the cable service attribute <b>non-ds-bonded downstream-type bonding-disabled</b>, and cable fiber node.</p> <p>Workaround: There is no workaround.</p>
CSCta60033	<p>Symptoms: Traceback and spurious memory access is observed due to failover of a PRE.</p> <p>Workaround: There is no workaround.</p>
CSCta67740	<p>Symptoms: PC/PCMM gates remain stuck on the Cisco CMTS after PRE or line card switchover.</p> <p>Conditions: This issue is observed when the cisco CMTS is running more than 300 PC/PCMM calls and the PRE or LC switchover is triggered.</p> <p>Workaround: Manually delete the gates using the <b>test packetcable gc gate-delete</b> command.</p> <p>However, there is no workaround in the Cisco IOS Release 23BC, where the above command fails.</p>
CSCta87238	<p>Symptoms: The <b>cable load-balance exclude list</b> displays unpredictable results.</p> <p>Conditions: This issue occurs when you:</p> <ol style="list-style-type: none"> <li>1. Start without the <b>cable load-balance exclude list</b>.</li> <li>2. When <b>cable load-balance exclude modem aaa.bbbb.cccc</b>, <b>cable load-balance exclude oui aaa.bb</b>, and <b>no cable load-balance exclude modem aaa.bbbb.cccc</b> commands are entered."</li> </ol> <p>The <b>cable load-balance exclude oui</b> configuration is removed, but the exclude modem configuration still remains.</p> <p>Workaround: Enter the <b>exclude oui aaa.bb</b> configuration before entering the <b>exclude modem aaa.bbbb.cccc</b> configuration.</p>
CSCtb04101	<p>Symptoms: A positive integer value is returned for the MB object <b>docsIfCmtsChannelUtUtilization</b> (OID 1.3.6.1.2.1.10.127.1.3.9.1.3) of the Cisco uBR10000 series universal broadband router with 5/1 HCCP protect interface when it is on standby.</p> <p>When a HCCP 5/1 protect card is in standby no traffic utilization should be reported.</p> <p>Conditions: This issue is observed on the Cisco uBR10000 series universal broadband router with Cisco IOS Release 12.3(23)BC4 having redundant ESR-PRE2 modular cable DOCSIS 3.0 configurations.</p> <p>Workaround: There is no workaround.</p>

Table 20 Resolved Caveats for Cisco IOS Release 12.3(23)BC9 (continued)

DDTS ID Number	Description
CSCtb23412	<p>Symptoms: There are no known symptoms for this issue.</p> <p>Conditions: This issue is very unlikely to occur. This issue occurs only if the device is in the wrong chain beyond the second position.</p> <p>Workaround: There is no workaround.</p>
CSCtb42127	<p>Symptoms: Multiple modular remote primary modems report majority or all of the modems offline because of more than one identical <b>downstream modular x/y/z rf-channel n</b> configurations in multiple domains.</p> <p>Conditions: This issue is observed on the Cisco uBR10000 series universal broadband router with Cisco IOS Release 12.3(23)BC4 running redundant ESR-PRE2 modular cable DOCSIS 3.0 configurations.</p> <p>Workaround: Remove the duplicate configurations from the unwanted interface by executing the <b>no downstream modular</b> command.</p> <p>It may also require the downstream modular configurations on all interface to be removed and reconfigured.</p>
CSCtb48785	<p>Symptoms: Remote narrow-band (NB) embedded media terminal adapters (eMTAs) drop offline after line card switch over (LCSO) if the modular host is on another card.</p> <p>Conditions: This issue is observed when:</p> <ul style="list-style-type: none"> <li>• The NB eMTAs have ongoing PacketCable calls</li> <li>• Dynamic service has the payload header suppression (PHS) enabled</li> <li>• The modular host is configured on another card</li> <li>• NB eMTAs drop offline only after LCSO</li> </ul> <p>Workaround: Configure modular host and MAC Domain host on the same cable line card.</p>
CSCtb57506	<p>Symptoms: The PXF crash displays the following message:</p> <pre>PXF DMA OQC at End of Descriptor With Non-Zero Continuation Bit</pre> <p>Conditions: This issue occurs on a Cisco uBR10000 series universal broadband router running Cisco IOS Release 12.3(23)BC5. It occurs under these conditions:</p> <ul style="list-style-type: none"> <li>• When Cisco IOS Netflow is configured.</li> <li>• There are many CM/CPEs on the Cisco CMTS and each CM/CPEs have several flows, that is, queues exist in the Cisco CMTS.</li> </ul> <p>Workaround: Disabling the Cisco IOS Netflow resolves the first condition for this issue.</p> <p>There is no workaround for the second condition.</p>
CSCtb63881	<p>Symptoms: The channel grouping domain (CGD) is lost after the line card and PRE switchover.</p> <p>Workaround: There is no workaround.</p>

**Table 20** *Resolved Caveats for Cisco IOS Release 12.3(23)BC9 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCtb86412	<p>Symptoms: When upstream frequency is changed from 35 Mhz to 38 MHz, cable modem reports about 7 db increment in transmission power.</p> <p>Conditions: This issue is observed on a Cisco uBR10000 series router with PRE2, and running Cisco IOS Release 12.3(23)BC4.</p> <p>Workaround: There is no workaround.</p>
CSCtb92591	<p>Symptoms: After a line card switchover, all downstream service flows are deleted.</p> <p>Workaround: There is no workaround.</p>
CSCtc03565	<p>Symptoms: The wavelength channel module (WCM) on the SPA may go offline after the PRESW.</p> <p>Conditions: This issue occurs when multiple SPAs are present in the system.</p> <p>Workaround: There is no workaround.</p>
CSCtc11429	<p>Symptoms: The <b>show interface cable x/y/z cable-monitor cam</b> command displays an incorrect hit counter on the last upstream when using an interface with eight upstreams.</p> <p>Conditions: This issue is observed when using the cable monitor on an interface that has cable upstream max-ports set to 8. The hit counters display 0 for the eighth upstream if the cable monitor is not configured. If the cable monitor is configured to monitor a cable modem using a MAC address on that interface, the eighth upstream shows a random number of hits.</p> <p>Workaround: There is no workaround.</p>
CSCtc17575	<p>Symptoms: The <b>cable privacy hotlist cm &lt;a.a.a&gt;</b> command does not block CMs from coming online.</p> <p>Conditions: This issue occurs when the modems do not have the appropriate certificates.</p> <p>Workaround: There is no workaround.</p>
CSCtc33526	<p>Symptoms: When the configuration changes the non-primary channel on the peer protect card to primary channel, and added it to the MAC Domain with active multicast sessions, it causes the peer protect card to crash.</p> <p>Conditions: This issue is observed when the channel is a non-primary channel on the card, which means some wideband channel includes the RF channel on the same fiber node with the primary channels on the card.</p> <p>Workaround: Tear down the multicast session before changing the configuration and perform the Internet group management protocol (IGMP) join again after changing the configuration.</p>

## Open Caveats for Release 12.3(21a)BC9

Table 21 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(21a)BC9.

**Table 21** *Open Caveats for Cisco IOS Release 12.3(21a)BC9*

<b>DDTS ID Number</b>	<b>Description</b>
CSCek41611	<p>Symptom: The Cisco uBR10-MC5X20U line cards may experience a silent reload.</p> <p>Conditions: This issue was first observed on a PRE 2 processor module running Cisco IOS Release 12.3(13a)BC2.</p> <p>Workaround: Upgrade to Cisco IOS Release 12.2(33)SCB1.</p>
CSCsq35790	<p>Symptom: The Voice over IP (VoIP) packets of Session Initiation Protocol (SIP) are not recognized. The VoIP packets are assigned to normal Committed Information Rate (CIR) queue instead of Low Latency Queuing (LLQ).</p> <p>Condition: This issue is observed when “Max DS Latency” information is not included in Dynamic Service Change (DSC) message.</p> <p>Workaround: Configure “Max DS Latency” information on cable modem.</p>
CSCsr70184	<p>Symptom: Access to a gate is refused due to exceeded activity-count even when the subscriber has no gate assigned.</p> <p>Condition: This issue was observed when Packetcable was running.</p> <p>Workaround: Increase the activity count in the Gate-Set messages.</p>
CSCsr75525	<p>Symptom: Incorrect power values for Power Entry Modules (PEM) is displayed by the <b>show controllers clock-reference</b> command.</p> <p>While PEM0 + PEM1 should not be higher than 2400, a single PEM's power exceeds that value.</p> <p>Condition: This issue is seen when a Cisco uBR10012 TCC card is used. Re-seating the card does not solve the problem.</p> <p>Workaround: There is no workaround.</p>

## Resolved Caveats for Cisco 12.3(21a)BC9

Table 22 only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(21a)BC9.

Table 22 Resolved Caveats for Cisco IOS Release 12.3(21a)BC9

DDTS ID Number	Description
CSCse85652	<p>Symptom: Access to the Cisco IOS HTTP server is denied if the enable password is not configured.</p> <p>Conditions: This issue is seen in the following conditions:</p> <ul style="list-style-type: none"> <li>• Enable password is not present in the device configuration</li> <li>• Cisco HTTP server or Cisco HTTPS server is enabled</li> <li>• No other authentication mechanism such as Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access-Control System (TACACS+) or is configured to access the Cisco HTTP or Cisco HTTPS servers</li> </ul> <p>Workaround: The following workaround can be used:</p> <ul style="list-style-type: none"> <li>• Enable the authentication to the Cisco HTTP server or Cisco HTTPS server by configuring the enable password or enable secret commands to configure the password. Use the following steps to configure the enable password using the enable secret command: <ol style="list-style-type: none"> <li>1. Replace “mypassword” with the new password.</li> <li>2. For information on the differences on configuring the enable secret and enable passwords, refer to the <i>Cisco IOS Password Encryption Facts</i> at <a href="http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml">http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml</a></li> </ol> </li> <li>• Enable authentication mechanisms such as RADIUS or TACACS+. For information on configuration, refer to <a href="http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml">http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml</a></li> <li>• Disable the Cisco HTTP server or the Cisco HTTPS server using <b>no ip http server</b> and <b>no ip http secure-server</b> commands.</li> </ul>
CSCsg00102	<p>Symptoms: The SSLVPN service stops accepting any new SSLVPN connections.</p> <p>Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.</p> <p>Workaround: Clear TCP connections using the <b>clear tcp tcb</b> command.</p>
CSCsh97579	<p>Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels</a></p>

**Table 22 Resolved Caveats for Cisco IOS Release 12.3(21a)BC9 (continued)**

DDTS ID Number	Description
CSCsi13344	<p>Symptom: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.</p> <p>The Cisco Security Response is posted at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http">http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http</a></p> <p>Conditions: See “Additional Information” section in the posted response for further details.</p> <p>Workarounds: See “Workaround” section in the posted response for further details.</p>
CSCsj10593	<p>Symptom: A terminating gateway (TGW) that is configured for Cisco ISDN Interconnect for Voice Gateways Solution may crash.</p> <p>Conditions: This occurs when the ISDN test call interface Serial1:23 22222 is issued at the Call Starter. This happens with Switch Types: OGW: primary-ni TGW: primary-dms100.</p> <p>Workaround: There is no workaround.</p>
CSCsk64158	<p>Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp</a></p>
CSCsm27071	<p>A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:</p> <ul style="list-style-type: none"> <li>• The configured feature may stop accepting new connections or sessions.</li> <li>• The memory of the device may be consumed.</li> <li>• The device may experience prolonged high CPU utilization.</li> <li>• The device may reload. Cisco has released free software updates that address this vulnerability.</li> </ul> <p>Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip</a></p>

**Table 22** *Resolved Caveats for Cisco IOS Release 12.3(21a)BC9 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCso04657	<p>Symptoms: SSLVPN service stops accepting any new SSLVPN connections.</p> <p>Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.</p> <p>Workaround: There is no workaround.</p>
CSCso90058	<p>Symptoms: The Multilayer Switch Feature Card (MSFC) crashes with RedZone memory corruption.</p> <p>Conditions: This occurs while processing an Auto-RP packet with Network Address Translation (NAT) enabled.</p> <p>Workaround: There is no workaround.</p>
CSCsq31776	<p>Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels</a></p>
CSCsr48745	<p>Symptom: Some modems go offline, after the linecard switchover or revertback, and “upstream phy register” shows late map issue.</p> <p>Condition: This occurs when the “dynamic map-advance safety” is configured with a small value.</p> <p>Workaround: Increase the value of “dynamic map-advance safety” or use static map-advance.</p>
CSCsr72301	<p>Symptom: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.</p> <p>The Cisco Security Response is posted at the following link: <a href="http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http">http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http</a></p>

**Table 22 Resolved Caveats for Cisco IOS Release 12.3(21a)BC9 (continued)**

DDTS ID Number	Description
CSCsr74034	<p>Symptom: Ironbus restarts have been observed on the Cisco uBR10012 router due to ironbus link status 0x1180 errors. You observe the following messages in the PRE log:</p> <pre data-bbox="574 436 1474 653"> ----- 811468: Jun 17 03:10:17.233 UTC: slotindex is 8. 811469: Jun 17 03:10:17.233 UTC: IB Link status: 00001180 811470: Jun 17 03:10:17.233 UTC: %C10KEVENTMGR-1-IRONBUS_FAULT: Ironbus Event 5/0, Restarting Ironbus 811471: Jun 17 03:10:17.645 UTC:%C10KEVENTMGR-1-IRONBUS_SUCCESS: Ironbus Event 5/0, Restart Successful ----- </pre> <p>The ironbus link status 0x1180 error will trigger an line card switchover on uBR10012s configured with N 1 redundancy. The ironbus restart is fast enough to keep modems online and has negligible affect to customers on uBR10012s without N+1 redundancy.</p> <p>Conditions: This ironbus link status 0x1180 error has only been observed on slot 5/0 with the following hardware configuration. - Working Cisco uBR10-MC520H line card in slot 5/0 (the problem has not been reported on the Cisco uBR10-MC520U/S cards) - Active PRE2 in slot A (the problem has not been reported on a PRE1) Cisco Systems is still investigating the root cause of the ironbus link status 0x1180 error.</p> <p>Workaround: There are two workarounds for ironbus link status 0x1180 error 1. Use Active PRE2 in slot B 2. Do not use a Cisco uBR10-MC520H in slot 5/0 Customers should not RMA any equipment due to the ironbus link status 0x1180 error. Cisco Systems has not confirmed that this is a hardware issues and would need to identify the faulty hardware (for example, PRE2 processor module, Cisco uBR10-MC520H, chassis) if it is a hardware issue.</p>
CSCsr93439	<p>Symptom: On reverting after a linecard switchover, some upstream cable modems go offline and do not return online because the PHY is in error state. This was observed to occur with both, Cisco IOS Release 12.3(23)BC2 and Cisco IOS Release 12.3(23)BC3.</p> <p>Conditions: There are many upstream channels in no-shut state in the Cisco uBR10-5X20H linecard. This problem can occur on performing a switchover and reverting to the previous state.</p> <p>Workaround: Execute the <b>shutdown</b> and <b>no shutdown</b> commands to bring the cable modems online.</p>
CSCsu36225	<p>Symptom: Two upstream ports on the same PHY receiver of a Cisco uBR10-MC5X20H line card show signal-to-noise ratio (SNR) degradation of about 10 dB.</p> <p>Condition: This occurs due to ingress-noise cancellation.</p> <p>Workaround: There is no workaround.</p>

**Table 22**      **Resolved Caveats for Cisco IOS Release 12.3(21a)BC9 (continued)**

DDTS ID Number	Description
CSCsu95526	<p>Symptom: Cable modems go offline due to a very low signal-to-noise ratio (SNR) value when PRE-Equalization is enabled.</p> <p>Conditions: This issue is observed when the modulation profile IUC1 (request) burst size is 1 minislot.</p> <p>Workaround: Calculate the request (IUC1) burst size based on the modulation profile, symbol rate, and minislot size configuration. Make sure that request burst profile is at 2 minislot in duration.</p>
CSCsv04901	<p>Symptom: When the Cisco uBR10-MC5X20H line card is in normal operation condition, modems on one or a few upstreams get into a bad state, and all modems on the affected upstreams go offline, while other upstreams are still functioning.</p> <p>Condition: There is traffic on the upstreams. This affects only the Cisco uBR10-MC5X20H line cards on all releases.</p> <p>Workaround: Execute the <b>shut</b> and <b>no shut cable interface</b> commands on the affected upstreams.</p>
CSCsv30595	<p>Symptoms: The OSPF process may crash.</p> <p>Conditions: The OSPF crash may be seen when the router receives invalid OSPF messages.</p> <p>Workaround: There is no workaround.</p>
CSCsv34656	<p>Symptom: A particular malformed OSPF message may cause the device to crash or operate unpredictably. The possible effects of this are:</p> <ul style="list-style-type: none"> <li>• The router may crash.</li> <li>• Routing loops may form in the network.</li> <li>• OSPF may controls the CPU and drop adjacencies.</li> <li>• The <b>show ip ospf database net</b> command output displays unwanted lines.</li> </ul> <p>Conditions: This is seen when the OSPF receives a malformed OSPF message.</p> <p>Workaround: None. Using OSPF authentication may help mitigate this issue.</p>
CSCsv73509	<p>Symptom: Terminal Access Controller Access-Control System (TACACS) or XTACACS is broken.</p> <p>Conditions: This occurs when <b>no aaa new-model</b> command is configured and the authentication happens through the local when TACACS is configured. This happens for the exec users under vty configuration.</p> <p>Workaround: There is no workaround.</p>

**Table 22 Resolved Caveats for Cisco IOS Release 12.3(21a)BC9 (continued)**

DDTS ID Number	Description
CSCsw24700	<p>Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:</p> <p>Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.</p> <p>SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.</p> <p>Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link:  <a href="http://www.cisco.com/en/US/products/csa/cisco-sa-20090325-webypn.html">http://www.cisco.com/en/US/products/csa/cisco-sa-20090325-webypn.html</a></p>
CSCsw43997	<p>Symptoms: A customized cable modulation profile causes the modems to fall offline and register on a different upstream.</p> <p>Workaround: 1) Reduce the preamble length of the station ranging burst</p> <pre data-bbox="574 835 1419 940">cable modulation-profile 123 initial 5 34 0 48 qpsk scrambler 152 no-diff 256 fixed cable modulation-profile 123 station 5 34 0 48 16qam scrambler 152 no-diff 256 fixed</pre> <p>2) Set both initial and station ranging bursts to 16QAM.</p> <pre data-bbox="574 989 1419 1094">cable modulation-profile 123 initial 5 34 0 48 16qam scrambler 152 no-diff 392 fixed cable modulation-profile 123 station 5 34 0 48 16qam scrambler 152 no-diff 392 fixed</pre>
CSCsw81745	<p>Symptoms: Modems may go offline with tdma-atdma mode if the upstream is configured with minislot size as 4.</p> <p>Condition: This issue is seen when the upstream in configured with minislot size 4.</p> <p>Workaround: Change the mini-slot size to 2.</p>
CSCsx70889	<p>Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>This advisory is posted at  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels</a></p>

**Table 22** Resolved Caveats for Cisco IOS Release 12.3(21a)BC9 (continued)

DDTS ID Number	Description
CSCsy15227	<p>Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.</p> <p>There are no workarounds that mitigate this vulnerability.</p> <p>This advisory is posted at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy</a></p>
CSCsy56311	<p>Symptom: The CPE fails to acquire an IP address using Dynamic Host Configuration Protocol (DHCP).</p> <p>Conditions: This issue is seen when the CPE host is first connected to a wrong CM and fails to acquire an DHCP address. If the CPE is connected later to the correct CM, the CPE still does not acquire the IP address.</p> <p>Workaround: Execute <b>clear cable host</b> command on the MAC address of the CPE.</p>

## Open Caveats for Release 12.3(23)BC8

Table 23 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(23)BC8.

**Table 23** Open Caveats for Cisco IOS Release 12.3(23)BC8

DDTS ID Number	Description
CSCek30621	<p>Symptoms: Wideband modem downstream throughput rate is not yet supported.</p> <p>Conditions: The packet per second and bits per second throughput rate for each wideband CM downstream service flow is not available. This affects both the <b>show cable modem Cx/y/z service-flow [counters   verbose]</b> and <b>show cable modem a.b.c.d qos</b> commands.</p> <p>Workaround: There is no workaround.</p>
CSCsr59753	<p>Symptoms: The Cisco IOS Release 12.3(23)BC2 mixed docsis mode (atdma-tdma) can only achieve 40 Unsolicited Grant Service (UGS) for an upstream. But, Cisco IOS Release 12.3(17b)BC9 can achieve 48 UGS flows.</p> <p>Conditions: This issue occurs with mixed DOCSIS mode and modems.</p> <p>Workaround: There is no workaround.</p>
CSCsu33316	<p>Symptoms: The cable line card crashes after the execution of the <b>clear arp</b> and <b>clear cable modem delete</b> commands.</p> <p>Conditions: The condition is unknown.</p> <p>Workaround: There is no workaround.</p>

Table 23 Open Caveats for Cisco IOS Release 12.3(23)BC8

DDTS ID Number	Description
CSCsu77588	<p>Symptoms: The online cable modems go offline with no alert or log message.</p> <p>Conditions: This issue is only related to Cisco uBR10-MC5X20U cards on the Cisco uBR10012 platform. This issue is similarly seen in Cisco uBR10-MC5X20H cards.</p> <p>Workaround: Executing the shut or the no-shut commands on the affected interfaces or power-cycling the cable line card solves the problem.</p>
CSCsv14196	<p>Symptoms: Secondary PRE crashes when Dynamic Bandwidth Selection (DBS) function is applied to wideband interface.</p> <p>Conditions: The issue is seen on a PRE-2 running Cisco IOS Release 12.3(23)BC2.</p> <p>Workaround: There is no workaround.</p>
CSCsv53276	<p>Symptoms: The <b>show controller modular-cable</b> command shows that RF channel 0 become unknown after hw-module reset.</p> <pre>SPA IP address = 192.168.5.1 SPA MAC Addr = 0012.001A.67D7 QAM MOD ANNEX TKB Interval Rate adjust State 0 Unknown Unknown 0 1 Enabled ====&gt; unknown 1 QAM 256 Annex B 2423 132 Enabled 2 QAM 256 Annex B 2423 132 Enabled 3 QAM 256 Annex B 2423 132 Enabled</pre> <p>Conditions: This issue occurred after an issue of the <b>hw-module reset</b> command and the <b>show diagnostic</b> command. This causes all wideband modems go to NB.</p> <p>Workaround: Reload the router to correct the issue.</p>
CSCsv58913	<p>Symptom: Address resolution fails for downstream packet when running cable <b>source-verify dhcp</b> command.</p> <p>Condition: This issue occurs when a Cisco uBR Series router configured to verify a CPE device's IP address to MAC address resolution, through the use of DHCP LEASEQUERY messages instead of using ARP.</p> <p>Workaround: Temporarily allow downstream ARP resolution using cable bundle interface commands, <b>cable arp</b> and <b>cable proxy-arp</b>.</p>
CSCsv59917	<p>Symptoms: The customer logs reported loss of configurations of the SPAs installed on the Cisco Wideband SIP.</p> <p>Condition: The issue occurred on two SPAs installed in the Cisco Wideband SIP. The SPA1/0/1 lost all its configurations, including its IP and MAC addresses, and all the RF channel configurations. The SPA1/0/0 retained the IP and MAC addresses but lost the RF channel configurations. Recovery measures such as including PRE switchover, hw-module reset, unprovision or reprovision the SPAs were attempted.</p> <p>Workaround: Reloading the router is the only way to recover.</p>

**Table 23**      **Open Caveats for Cisco IOS Release 12.3(23)BC8**

DDTS ID Number	Description
CSCsv85159	<p>Symptom: The upstream ports configured as HCCP protect shows the link down on the minor alarm instead of at the informative level when executing <b>show facility-alarm status</b> command .</p> <p>Condition: This issue is seen when the cable line card is configured as HCCP protect and the router is running a later release than Cisco IOS Release 12.3(23)BC2.</p> <p>Workaround: There is no workaround.</p>
CSCsv94281	<p>Symptoms: The throughput of modular cable or the wideband interface is larger than the real value after a PRE processor module switchover. After 10-20 minutes, the throughput recovers automatically. This issue is seen on legacy interface on the routers running Cisco IOS Release 12.3(23)BC. This is displayed while executing <b>show interface</b> command</p> <p>Conditions: This issue is seen during a PRE processor switchover.</p> <p>Workaround: There is no workaround.</p>
CSCsw14622	<p>Symptoms: For deleted service flows associated with PCMM calls the last character in the Service Class Name field is dropped in SAMIS records as well as in the SNMP MIB object "docsQoSServiceFlowLogServiceClassName".</p> <p>Conditions: This issue is seen when the dynamic service flows associated with PCMM calls are deleted. The last character is missing from the service class name in the MIB object "docsQoSServiceFlowLogServiceClassName" and SAMIS records</p> <p>Workaround: There is no workaround.</p>
CSCsw33866	<p>Symptoms: Both the working card and protect card are active.</p> <p>Conditions: This issue is seen when a line card switchover happens from 5/0 to 5/1. After synchronization, shut down the 5/0/2 interface, and then revert from 5/1 to 5/0. If the 5/0/2 interface is not shut down, and after the suspend timer interval expires, both 5/0 and 5/1 are active.</p> <p>Workaround: Do not shut down an active protect interface. If both the cards (working and protect) are active, reset the protect card.</p>
CSCsw49188	<p>Symptoms: Cable metering fails and enters a “hung” state.</p> <p>Conditions: The issue happens when the “ip tcp timestamp” option is configured globally.</p> <p>Workaround: Do not use the “ip tcp timestamp” option.</p>
CSCsw51992	<p>Symptom: Invalid or corrupt values seen for OctetsPassed and PacketsPassed fields in SAMIS records.</p> <p>Conditions: This issue is seen in CMTS with wideband SPA configured when querying the service flow counters using SAMIS, snmp or executing show commands.</p> <p>Workarond: There is no workaround.</p>

**Table 23 Open Caveats for Cisco IOS Release 12.3(23)BC8**

DDTS ID Number	Description
CSCsw68704	<p>Symptoms: The wideband modem can get to wb-online state.</p> <p>Conditions: This is seen if a <b>shutdown</b> command is executed followed by a <b>no shutdown</b> command on an active protect interface.</p> <p>Workaround: Do not execute the <b>shutdown</b> command an active protect interface.</p>
CSCsx45807	<p>Symptoms: The IPDR can trigger high RP CPU utilization when entries in the service flow log table time-out, and the data is written to the disk.</p> <p>Conditions: This issue is seen when IPDR uses the file system for the deleted service flow information if the cable <b>sflog</b> command is configured such that the entry-duration is too short or the number of entries is too low.</p> <p>Workaround: Prevent storage of deleted service flows on the disk by using the recommended configuration of the cable <b>sflog</b> command. The entry duration should be at least four times the metering interval and the max-entry should be large enough to store the deleted flows that exist in a metering interval.</p> <pre data-bbox="574 806 1227 856">cable metering destination &lt; retries&gt; 15 non-secure cable sflog max-entry 30000 entry-duration 3600</pre> <p>With the metering interval at 15 minutes, the service flow log should be at least 1 hour or 3600 seconds. The high CPU occurs when the file system is full, and attempts to write are continued .</p>
CSCsx54955	<p>Symptoms: Multimedia Terminal Adaptor (MTA) CMs are not accessible from the CMTS or Internet because the ARP entry is replaced with an all-zero MAC address. Hence it is not accessible when a crafted packet is sent.</p> <p>Conditions: This issue occurs when a crafted packet is sent to the CMTS, causing the CMTS to use the wrong MAC address for the ARP table.</p> <p>Workaround: Execute the <b>cable source-verify dhcp server x.x.x.x</b> command, where x.x.x.x is your DHCP server, and use cable arp filter to limit the potential ARP storm.</p>
CSCsx56465	<p>Symptoms: Wideband CMs using a stats index are not managed by the modular-host. This causes two modems using the same Blaze header stats index, thus leading to incorrect downstream traffic statistics on these modems.</p> <p>Conditions: This issue occurs when there are wideband modems in the w-online state and a change is made to the downstream channel ID of the MAC domain host of these wideband modems.</p> <p>Workaround: There is no workaround.</p>
CSCsx79870	<p>Symptoms: Modifying the <i>second-choice-channel-width</i> has no affect on the configuration even though the cable upstream channel-width command accepts the input.</p> <p>Conditions: This issue is seen in Cisco IOS Release 12.3BC.</p> <p>Workaround: Modify the <i>first-choice-channel-width</i>, and then reconfigure the first and second choice.</p>

**Table 23**      **Open Caveats for Cisco IOS Release 12.3(23)BC8**

DDTS ID Number	Description
CSCsy13870	<p>Symptoms: When configuring cable upstream threshold cnr-profile snr-profile, the parser shows and accepts the second threshold value. It does not give an error message, and does not display the configuration with only the first threshold value.</p> <p>Conditions: This issue is seen while configuring the CNR and SNR thresholds for modulation profiles.</p> <p>Workaround: Either enter any valid threshold value or “0” to bypass.</p>
CSCsy16511	<p>Symptoms: When applying modulation profiles to an upstream port, the modulation profiles are re-ordered, high performance to robust/low performance. Modifying the order of the modulation or symbol rate on the profile does not happen.</p> <p>Conditions: If the signal-to-noise ratio (SNR) threshold is set at 25 with a hysteresis of 2 (bypassing all FEC), the modulation on the upstream will be QPSK until the SNR falls below 25 dB where it will change to 16-QAM. When the SNR reaches 27 dB (25 dB + 2 dB), the modulation reverts to QPSK. When a line card switchover is performed, the modulation profiles are re-ordered on the protect card.</p> <p>Workaround: Remove and re-apply modulation-profile configuration on the upstream port after modifying the modulation profiles.</p>
CSCsy16934	<p>Symptoms : A wideband CM cannot go into the w-online state after resetting both the working line card (guardian line card) and the protect line card and after the working line card reboots and becomes active.</p> <p>Conditions: This issue is seen while resetting the working line card which is the guardian line card and when the working line card reboots first and becomes active.</p> <p>Workaround: Remove and reconfigure the guardian configuration.</p>
CSCsy18380	<p>Symptoms: All CMs on adjacent downstreams are offline. The adjacent downstream ports are 0 and 1, or 2 and 3, or 4.</p> <p>Conditions: The downstream ports that share JIB may be nonfunctional if the JIB that services both downstream ports is locked.</p> <p>Workaround: Reload the cable line card.</p>
CSCsy23149	<p>Symptoms: The MIB object “entPhysicalName” for theCisco uBR10012 router does not display the values correctly. The values as displayed as slot 0/0/0 and slot 0/1/0 for the PRE processor modules instead of being displayed as 0A and 0B from left to right. Similarly, the MIB object “entPhysicalName” returns slot x/x/x (for example, 1/0/0) instead of the values displayed in the device.</p> <p>Conditions: This issue occurs while querying the MIB object “entPhysicalName”.</p> <p>Workaround: There is no workaround.</p>

**Table 23 Open Caveats for Cisco IOS Release 12.3(23)BC8**

DDTS ID Number	Description
CSCsy55647	<p>Symptoms: A crash is observed on the ESR-PRE2 processor module. The crash information logs may contain the following:</p> <pre data-bbox="573 390 1487 527">%UBR10K-6-US_SFID_INCONSISTENCY: US-SF found: SFID xxxx, type 0, sid 0(yyyy), MAC aaaa.aaaa.aaaa(bbbb.bbbb.bbbb), prim_sid xxx(yyy)CMD: 'no cable service attribute voice-enabled downstream-type HA-capable'</pre> <p>Conditions: This issue is seen in Cisco IOS Release 12.3(23)BC4.</p> <p>Workaround: There is no workaround.</p>
CSCsy55849	<p>Symptoms: The show controller modular-cable command output displays invalid voltage measurement readings for the 24 rf-channel SPA.</p> <p>Conditions: This is seen on the 24 rf-channel SPA.</p> <p>Workaround: Re-execute the show controller modular-cable command.</p>
CSCsy59457	<p>Symptoms: After a reload, <b>cable metering source-interface FastEthernet0/0/0</b> is not present at the running configuration, although <b>cable metering filesystem disk0:cpe-list-suppress</b> and <b>cable metering source-interface FastEthernet0/0/0</b> were configured.</p> <p>Conditions: This issue is seen only in Cisco IOS release versions on the PRE2 processor module and not in Cisco IOS releases versions of the Cisco uBR7200 router.</p> <p>Workaround: There is no workaround.</p>
CSCsy93613	<p>Symptoms: The Dynamic Message Integrity Check (DMIC) code is being corrupted due to a DHCP packet.</p> <p>Conditions: This issue seen on PRE2 processor module running Cisco IOS Release 12.3(23)BC2.</p> <p>Workaround: There is no workaround.</p>
CSCsz25605	<p>Symptoms: The Gigabit Ethernet interface on an ESR-1GE may fail to send packets.</p> <p>Conditions: This might be seen just after executing online insertion and removal (OIR) of an ESR-1GE with low rate.</p> <p>Workaround: Execute the <b>hw-module slot reset</b> command.</p>
CSCsz49382	<p>Symptoms: The cable modems are not able to access the Layer 3.</p> <p>Conditions: This issue is seen on Cisco UBR10-MC5X20U-D card on Cisco UBR10012 router running Cisco IOS Release 12.3(23)BC4.</p> <p>Workaround: Power off or power on cable line card.</p>

**Table 23**      **Open Caveats for Cisco IOS Release 12.3(23)BC8**

DDTS ID Number	Description
CSCsz51198	<p>Symptoms: The guardian line card does not synchronize with the new key to the standby line card, when a key is renewed for a wideband multicast sid,. This causes the wrong key to be sent to a wideband CM for that multicast sid after the guardian line card switches over.</p> <p>The information is not synchronized to the standby line card when the guardian line card assigns an index to a modular-cable multicast sid and key. It may reassign, the same key after a switchover.</p> <p>If the index of a remote guardian line card is not rightly made free for a modular-cable multicast sid and key, This could cause an index leak for the remote guardian line card and the information is not synced to the standby for both local and remote line cards. An index leak may happen if the guardian line card switches over.</p> <p>When an modular-cable interface is shut or removed from a Channel Grouping Domain (CGD), indexes are not cleaned up on standby guardian line card causing an index leak if the guardian switches over.</p> <p>Condition: This is seen after a guardian line card switchover.</p> <p>Workaround: There is no workaround.</p>
CSCsz56059	<p>Symptoms: The <b>cable dynamic-secret lock</b> command does not lock the rogue modem to 10kbps upstream or 10kbps upstream /downstream profile. The <b>show cable modem &lt;mac of rogue modem&gt; qos</b> command reports 0/0 kbps upstream/downstream rates for the same modem after the same modem reboots or resets.</p> <p>Conditions: The issue has been observed on Cisco uBR10012 router with PRE2 processor module running Cisco 12.3(23)BC4 with <b>cable dynamic-secret lock</b> command configured under the cable interface.</p> <p>Workaround: There is no workaround.</p>
CSCsz60401	<p>Symptoms: The following SPA bus error and Jacket watchdog reset is displayed on a Cisco Wideband SIP crashinfo:</p> <pre data-bbox="613 1304 1214 1409">SPI FPGA: TIB SPA1 Bus Error [1/16] Machine Check Error, can be ECC or Watchdog.. ECC 1 bit errors since last time we cleared = 0 ECC 1 bit errors while up (total) = 0</pre> <p>Conditions: This issue is seen when Cisco Wideband SPA power is shutdown and if power supply violation is watched by power management hardware to protect components on SPA.</p> <p>Workaround: There is no workaround.</p>
CSCsz85345	<p>Symptoms: When the CMTS SNMP MIB objects “docsIfCmtsCmStatusValueLastUpdate” and “sysUpTimeInstance” are calculated, the CM online time as reported by a few CMs seems larger than the actual uptime of the CM than when reported if polled directly from the CM.</p> <p>Conditions: The issue was reported only for a few hundred modems out of few millions.</p> <p>Workaround: There is no workaround.</p>

**Table 23** Open Caveats for Cisco IOS Release 12.3(23)BC8

DDTS ID Number	Description
CSCsz92784	<p>Symptoms: IPDR export records do show an increment in the downstream counters for some cable modems. The upstream counters are reported correctly by IPDR.</p> <p>Conditions: This is observed in routers running Cisco IOS Release 12.3(23)BC4 and in Cisco IOS Release 12.3(21)BC.</p> <p>Workaround: Reset the cable modem or use snmp poll to retrieve downstream and upstream data for a cable modem.</p>
CSCsz98503	<p>Symptoms: Multiple CMs go offline for a short time on a random upstream port. This is seen as a spike of the error per second rate or by a MER drop and by a decrease in docsIfSigQUnerrored.</p> <p>Conditions: This is seen on a Cisco uBR10012 router with uBR10-MC5x20H cards. The issue is not seen on Cisco uBR7246VXR router.</p> <p>Workaround: There is no workaround.</p>
CSCta03544	<p>Symptoms: The interfaces using frequency stacking may get dropped up to 10 dB in the average MER readings of <b>show controllers cable</b> command.</p> <p>Conditions: This is seen in routers running Cisco IOS Release 12.3(23)BC7.</p> <p>Workaround: Remove the frequency stacking or remove the frequency on the unused upstream.</p>
CSCta03992	<p>Symptoms: DOCSIS Set-Top Gateway (DSG) statistics does not show the modular cable interfaces Downstream Channel Descriptor (DCD) counters.</p> <p>Conditions: This occurs in normal conditions.</p> <p>Workaround: There is no workaround.</p>
CSCta18008	<p>Symptoms: The modems on a specific line card cannot come online after upgrading to Cisco IOS Release 12.3(23)BC4.</p> <p>Conditions: This following message is seen in the logs report the message:  <pre>%PXF_DMA-3-IRONBUS_NOTRUNNING: Data path to slot 5/0 failed to synchronize.</pre> </p> <p>Workaround: There is no workaround.</p>

## Resolved Caveats for Release 12.3(23)BC8

Table 24 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(23)BC8.

**Table 24 Resolved Caveats in Cisco IOS Release 12.3(23)BC8**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh40309	<p>The burst is not being displayed during a modem upstream (US) trace with Cisco Broadband Troubleshooter (CBT) Version 3.2 when pre-equalization is configured on the US port.</p> <p>This issue occurs only on the Cisco uBR10-MC5X20S and Cisco uBR10-MC5X20U cards when pre-equalization (equalization-coefficient) is configured.</p> <p>Workaround: Do not configure the pre-equalization feature. Note that this feature is off by default.</p>
CSCsh97579	<p>Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels</a></p>
CSCsq31776	<p>Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding. Cisco has released free software updates that address this vulnerability. This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels</a></p>
CSCsu08256	<p>Symptoms: The Cisco uBR10-MC5X20H card reloaded during forced line card failover.</p> <p>Conditions: This is seen in the Cisco uBR10-MC5X20H.</p> <p>Workaround: There is no workaround.</p>
CSCsv88650	<p>Symptoms: Modems on a modular interface suffer long-time recovery time or even fall offline after switchover or revertback.</p> <p>Conditions: This only affects Cisco uBR-MC5X20S/U card as the active card. It affects modems on the modular interface and is more visible for Annex A modulation type.</p> <p>Workaround: There is no workaround.</p>
CSCsw29191	<p>Symptom: When Three Way Calling (TWC) is used, the admitted service flow of the on-hold side still has traffic going through.</p> <p>Conditions: This is seen in three-way calling when one side is on hold. This is seen in Cisco IOS Release 12.3(23)BC and Cisco IOS Release 12.2(33)SCB release.</p> <p>Workaround: There is no workaround.</p>
CSCsw49606	<p>Symptoms: A cable line card crash may occur if a test cable dcc command is executed on a 2.0 modem, move it from an ATDMA upstream to a TDMA upstream (with fragmentation disabled).</p> <p>Condition: The issue is seen in routers running Cisco IOS Release 12.3(23)BC4.</p> <p>Workaround: There is no workaround.</p>

Table 24 Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)

DDTS ID Number	Description
CSCsw89288	<p>Symptoms: The <b>show interface cable x/y/z sid</b> command shows null MAC address and null IP address SID entries. The <b>show cable modem summary total</b> command reports many more offline modems than are actually offline.</p> <p>Conditions: This was first observed in Cisco IOS Release 12.2(33)SCB.</p> <p>Workaround: Clear the offline modems using the <b>clear cable modem offline delete</b> command. This issue is cosmetic.</p>
CSCsx23893	<p>Symptoms: Replacing an Cisco uBR10-MC5X20S/U/H with another Cisco uBR10-MC5X20S/U/H causes modems to drop offline and generate a console error message similar to the following:</p> <pre>ERROR: 1/0/0 rf-channel 0: already hosted under Ca5/1/1</pre> <p>The message indicates that an attempt was made to add the RF channel on the modular cable controller in slot 1, subslot 0, bay 0 to another the MAC domain when it was already configured for MAC Domain 1 on the cable line card in slot 5, subslot 1.</p> <p>Conditions: The problem occurs when the OIR-compatibility feature is invoked to preserve a line card configuration across an OIR operation when the line card configuration contains remote modular cable downstreams and N+1 redundancy configured. The compatibility feature is only invoked when a change of card type is detected. Replacing an Cisco uBR10-MC5X20 with the same card type does not cause the problem.</p> <p>Workaround: There are no workaround.</p>
CSCsx48561	<p>Symptoms: The Cisco Broadband Troubleshooter trace window appears to show incorrect data when triggering an upstream by CM MAC address. The MIB object "server% getmany -v2c ccsSpectrumDataPower" returns values that when graphed do not show the expected QAM haystack. This MIB does not provide data until the CMTS is first configured appropriately via SNMP sets.</p> <p>Conditions: This issue occurs in upstream frequency stacking and configured MAC domains.</p> <p>Workaround: Remove the frequency stacking and configured MAC domains.</p>
CSCsx53105	<p>Symptom: The Cisco uBR10012 router crashes with the following error:</p> <pre>PXF DMA Too Many Feedback Context Writes Error.</pre> <p>Condition: The cause of the bug is a rare timing event inside the PXF complex. The issue occurred while sampling packets for weighted early random discard. The PXF complex may try to update a shared memory structure using direct memory access. If the write to the shared memory structure fails, then the PXF complex is forced to crash.</p> <p>Workaround: There is no workaround.</p>
CSCsx57029	<p>Symptoms: An incorrect MAC address or IP address is obtained when the <b>show cable mode [mac   ip] access-group</b> command is executed.</p> <p>Conditions: This is seen in Cisco IOS Releases 12.3(23)BC.</p> <p>Workaround: There is no workaround.</p>

**Table 24 Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)**

DDTS ID Number	Description
CSCsx63371	<p>Symptoms: The Cisco uBR10-MC5X20H line card crashes.</p> <p>Conditions: This issue occurs during a PRE processor module switchover.</p> <p>Workaround: There is no workaround.</p>
CSCsx64462	<p>Symptoms: Unintentional reset of the Cisco SIP-600 card can occur if the show controller command is executed and there is a Cisco Wideband SPA card that is currently in a state of initialization.</p> <p>Conditions: This is seen if there is a SPA in a Cisco SIP-600 card that is in the process of being initialized.</p> <p>Workaround: Do not execute the show controller command if there is a Cisco SIP-600 card with a SPA that is in the process of being initialized.</p>
CSCsx67030	<p>Symptoms: The following traceback is seen when getting docsIfDownstreamChannelEntry:</p> <pre data-bbox="613 787 1521 1182"> SLOT 5/0: 00:09:18: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x6061A388 reading 0x2B0 SLOT 5/0: 00:09:18: %ALIGN-3-TRACE: -Traceback= 6061A388 60334794 6061D31C 606200D0 60519EBC 60519538 6050A97C 6050AB9C SLOT 5/0: 00:09:18: %ALIGN-3-TRACE: -Traceback= 6061A390 60334794 6061D31C 606200D0 60519EBC 60519538 6050A97C 6050AB9C SLOT 5/0: 00:09:18: %ALIGN-3-TRACE: -Traceback= 6061A3B4 60334794 6061D31C 606200D0 60519EBC 60519538 6050A97C 6050AB9C SLOT 5/0: 00:09:18: %ALIGN-3-TRACE: -Traceback= 6061A3C8 60334794 6061D31C 606200D0 60519EBC 60519538 6050A97C 6050AB9C </pre> <p>Conditions: This is seen when the broadband innovation upconverter is used.</p> <p>Workaround: There is no workaround.</p>
CSCsx69554	<p>Symptoms: Frequency range overlapping occurs.</p> <p>Conditions: This is seen when <b>cable freq-range north-american/european</b> command is configured on the CMTS.</p> <p>Workaround: Do not configure the <b>cable freq-range north-american/european</b> command in global mode.</p>
CSCsx77543	<p>Symptom: If Dynamic Message Integrity Check (DMIC) is configured in conjunction with IPv6 enabled CMs, the PRE crashes with the following message:</p> <pre data-bbox="613 1549 1521 1780"> *** System received a Bus Error exception *** signal= 0xa, code= 0x8, context= 0x6493a1a4 PC = 0x60a49ad0, Cause = 0x420, Status Reg = 0x34008002 System Bootstrap, Version 12.0(20020314:211744) [REL-pulsar_sx.ios-rommon 112], DEVELOPMENT SOFTWARE Copyright (c) 1994-2002 by cisco Systems, Inc. Reset Reason Register = RESET_REASON_RESET_REG (0x76) C10000 platform with 1044480 Kbytes of main memory </pre> <p>Conditions: This issue is seen when DMIC is configured in conjunction to IPv6-enabled CMs.</p>

**Table 24 Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)**

DDTS ID Number	Description
CSCsx77548	<p>Symptoms: Configuring more than four upstream channels in one downstream may cause a crash on the CMTS.</p> <p>Conditions: This issue is seen while configuring more than four upstream channels in one downstream and when a UGS_AD service flow is used.</p> <p>Workaround: Do not configure more than four upstream channels in one downstream.</p>
CSCsx79753	<p>Symptoms: An error "%GENERAL-2-CRITEVENT: MRI Unlink Error: Cable", is seen in the system logs for different CMs.</p> <pre data-bbox="574 621 1414 877">%GENERAL-2-CRITEVENT: MRI Unlink Error: Cable6/0/3 cpe_info-&gt;name: Cable8/1/3 current sid: 1464 cpe_info-&gt;sid: 1922 current mri: 472 cpe_info-&gt;mri: 472 modem-&gt;mac_addr: 001a.ad90.be36 cpe_info-&gt;mac_addr: 001a.ada7.c1a6 Current IP address: 78.94.54.211 cpe_info-&gt;ipaddress: 10.80.64.206 cpe_info-&gt;next_slot: 1048576 cpe_sidinstp: 0x0 cpe_sidinstp-&gt;prim_sid: 65535 cpe_sidinstp-&gt;cm_macaddr: 0000.0000.0000</pre> <p>Conditions: This issue is seen on the Cisco uBR10012 router.</p> <p>Workaround: There is no workaround.</p>
CSCsx80261	<p>Symptoms: The MAC Domain x/y/z interface loses modular-cable configuration.</p> <p>Conditions: This is seen after a Cisco uBR100012 router bootup.</p> <p>Workaround: There is no workaround.</p>
CSCsy09861	<p>Symptoms: Upstream-and-downstream-related tables are not retrieved while querying via SNMP.</p> <p>Conditions: This issue is seen while quering via SNMP.</p> <p>Workaround: There is no workaround.</p>
CSCsy13775	<p>Symptoms: A wrong description on a facility alarm shows up for some upstream ports after resetting a modular-host line card. The wrong description means that “Physical Port Administrative State Down” shows up for some upstream ports even when those upstream ports are not administratively shut down.</p> <p>Similarly, a wrong description on a facility alarm shows up for some upstream ports after reloading a Cisco uBR10012 router. The wrong description means that “Physical Port Link Down” shows up for some upstream ports even when those upstream ports are up.</p> <p>Conditions: This issue only occurs on line cards with upstream max-ports 6 configured.</p> <p>Workaround: Execute the <b>shut</b> command followed by a <b>no shut</b> command on the upstream ports.</p>
CSCsy13889	<p>Symptoms: The minor alarm is raised for all upstream ports of an administratively shut down cable interface after a reload the Cisco uBR10012 router.</p> <p>Conditions: This issue is seen on a Cisco uBR10012 router with an administratively shut down cable interface running Cisco IOS Releases 12.3(17b)BC9, 12.3(23)BC2, and 12.3(23)BC6.</p>

**Table 24 Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)**

DDTS ID Number	Description
CSCsy15227	<p>Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.</p> <p>There are no workarounds that mitigate this vulnerability.</p> <p>This advisory is posted at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy</a></p>
CSCsy23311	<p>Symptom: The Cisco uBR10012 router experienced several crashes when upgrading from Cisco IOS Release 12.3(21a)BC6 to Cisco IOS Release 12.3(23)BC6.</p> <p>Conditions: This crashes have been found when upgrading from Cisco IOS Release 12.3(21a)BC6 to Cisco IOS Release 12.3(23)BC6.</p> <p>Workaround: There is no workaround.</p>
CSCsy29498	<p>Symptoms: For the Cisco uBR-10-MC5X20 NB CM with the primary channel on remote a Cisco Wideband SPA downstream interface, its toaster BPI index is reset to 0 after a line card switchover; thus the downstream traffic is not encrypted.</p> <p>Conditions: The condition is unknown.</p> <p>Workaround: There is no workaround.</p>
CSCsy31477	<p>Symptoms: A preamble length of 49 symbols causes an issue with a Broadband BCM3300 chip with H cards. Imposing the minimum 50 symbols preamble length as to IM and SM bursts still reports the same issue.</p> <p>Workaround: Execute a <b>shut</b> command followed by a <b>no shut</b> command on the interface or execute a <b>cable upstream shutdown</b> command or a <b>no cable upstream shutdown</b> command.</p>
CSCsy33540	<p>Symptom: The PRE processor module crashes after removing the policy map.</p> <p>Conditions: This has been seen on a Cisco uBR10012 router with PRE-3 processor module running Cisco IOS Release 12.3(21a)SB5 IOS.</p> <p>Workaround: Do not remove the policy map.</p>
CSCsy44819	<p>Symptoms: Bonding-capable CMs may take a long time to get to the w-online state, or possibly fail to get to the w-online state.</p> <p>Conditions: This issue is seen when the CMTS is configured to forward for a bonding-capable CM to a bonding-capable primary downstream channel, the CMTS randomly selects the target from the set of DS channels defined in the MAC Domain Downstream Service Group (MD-DS-SG). When complex fiber nodes are configured, it is possible that one or more of those channels are primary in a different DOCSIS MAC domain. In the event the upstream channels for that MAC domain are not available at the current fiber node, then the CM fails to initialize at the target frequency. Due to the random nature of the target DS selection, multiple failures are possible.</p> <p>Workaround: There is no workaround.</p>

**Table 24 Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsy52912	<p>Symptoms: The modem gets stuck in the init (io) state when both working and protect line cards are reset at almost the same time.</p> <p>Conditions: This issue is seen when both the working and protect line cards are reset.</p> <p>Workaround: Reset the working card using the hw-module subslot x/y command or do a switchover.</p>
CSCsy56311	<p>Symptom: The CPE fails to acquire an IP address using DHCP.</p> <p>Conditions: This issue is seen when the CPE host is first connected to a wrong CM and fails to acquire an DHCP address. If the CPE is connected later to the correct CM, the CPE still does not acquire the IP address.</p> <p>Workaround: Execute <b>clear cable host</b> on the MAC address of the CPE.</p>
CSCsy62148	<p>Symptoms: CM fails to get online.</p> <p>Conditions: This issue is seen when a CM begins initial-ranging on an upstream port, and reports a DOCID for a different MAC domain.</p> <p>The CMTS issues a downstream frequency override (DFO) to the downstream frequency of the hosting interface (for example, Cisco uBR10-MC5X20 line card) of the upstream port being used. In this event, the target downstream port is in an "rf-shutdown" state", and the DFO fails.</p> <p>Workaround: There is no workaround.</p>
CSCsy72398	<p>Symptoms: Due to the way the CMTS US scheduler is designed, the VoIP traffic from a single CMTS shows the tendency to get synchronized in time.</p> <p>Conditions: This issue is seen when multiple CMTSs are connected to the same DTI server, and the egress VoIP traffic from these CMTSs to get synched. This multi-CMTS VOIP synchronization causes the peak VoIP rate on the aggregation routers to the levels which default buffers cannot be handled.</p> <p>Workaround: If the UGS scheduling across US channels is randomized on a single CMTS, it may to resolve the issue.</p>
CSCsy73726	<p>Symptom: The cable metering options "flow-aggregate" and "cpe-list-suppress" get lost from the cable metering configuration if <b>cable metering data-per-session x timer y</b> is present.</p> <p>Condition: This is seen in <b>cable metering</b> command.</p> <p>Workaround: Re-configure the metering options "flow-aggregate" and "cpe-list-suppress" in the command.</p>

**Table 24 Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)**

DDTS ID Number	Description
CSCsy76287	<p>Symptoms: After the Cisco uBR10012 router is upgraded from Cisco IOS Release 12.3(13a)BC1 to Cisco IOS Release 12.3.(23)BC2, the advanced spectrum management feature does not work.</p> <p>Conditions: The SNR value goes below the first threshold and enters the second modulation as required. The issue occurs if a change is made to the first modulation, using the second threshold as reference. For example:</p> <pre>Router# cable upstream 0 threshold snr-profiles 22 5 Mar 5 17:13:48 M 16-QAM QPSK SNR 21&lt;22 CNR 21&lt;22 CFEC 11&gt;=10 &lt;&lt;CORRECT Mar 5 17:14:10 M QPSK 16-QAM SNR 24&gt;=8 CFEC 0&lt;=10 UnCFEC 0&lt;=1 &lt;&lt; WRONG, it \ should be SNR &gt;=25</pre> <p>Workaround: Disable the second threshold value <b>cable upstream 0 threshold snr-profiles 22 0</b> command.</p>
CSCsy79521	<p>Symptoms: The calculated upstream port utilization percentage on ports 1 to 3 is below the actual usage.</p> <p>Conditions: This is seen when more than one upstream port is active for a given MAC domain. The upstream utilization for the higher port numbers can be too low.</p> <p>Workaround: There is no workaround.</p>
CSCsy92263	<p>Symptom: When auto-negotiation is enabled, it takes long time (approximately 4~5 minutes) to link up the uplink port of half-height Gigabit Ethernet line card. This is seen after the execution of a <b>shut</b> command followed by a <b>no shut</b> command at the port. During the issue, Cisco uBR10012 router shows the port as up/up, but the switch connecting to the Cisco uBR10012 shows down/down.</p> <p>Conditions: This issue is seen in the following:</p> <ul style="list-style-type: none"> <li>• Auto-negotiation is enabled</li> <li>• Executing a <b>shut</b> command followed by a <b>no shut</b> command on Cisco uBR10012 router</li> <li>• Router running Cisco IOS Releases 12.3(23)BC6 and 12.3(23)BC7.</li> </ul> <p>Workaround: There is no workaround.</p>
CSCsy93250	<p>Symptoms: All the 65535 Blaze indices are used up.</p> <p>Conditions: This happens when the guardian is remote and there are multiple service flows per CM.</p> <p>Workaround: Use a local guardian.</p>
CSCsz01750	<p>Symptoms: The error message “%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: No cable queue” occurred on PRE2 processor module running Cisco IOS Release 12.3(23)BC6.</p> <p>Condition: This issue is seen in on PRE2 processor module running Cisco IOS Release 12.3(23)BC6.</p> <p>Workaround: There is no workaround.</p>

**Table 24 Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)**

DDTS ID Number	Description
CSCsz02830	<p>Symptoms: Online insertion and removal (OIR) compatibility fails when it tries to reconfigure the MAC domain with SPA channels 16-23 on the new card.</p> <p>Conditions: This is seen on OIR replacement of the Cisco uBR10-MC5X20 cards. The cleanup of SPA channels 16-23 does not happen properly.</p> <p>Workaround: There is no workaround.</p>
CSCsz05250	<p>Symptoms: When setting a CA certificate to “untrusted”, any CM that uses an issuer of the same name is rejected, including the legitimate modems.</p> <p>Conditions: The issue is found because of a newly created software “Haxorware” which generates these CA certificates that conflict with the existing CA certificates.</p> <p>Workaround: The recommended method is always to not allow self-signed certificates on the CMTS and explicitly set specific self-signed certificates to trusted. This is the “opt-in” model, rather than the “opt-out” model.</p>
CSCsz20091	<p>Symptoms: Modems using SPA modular-cable downstreams on the Cisco uBR10012 router cannot go past the init (io) state.</p> <p>Conditions: This is seen when multicast encryption is enabled. This issue occurs when a key index request for an encrypted multicast session from the MAC domain host line card to the wideband host line card fails. Such a failure can occur due to an inter-line card IPC drop.</p> <p>Workaround: The following steps can be used to recover from this error state:</p> <ol style="list-style-type: none"> <li>1. Remove <b>cable match address</b> from any bundle interface which has associated with the SPA.</li> <li>2. Reset the SPA.</li> <li>3. Re-enable <b>cable match address</b> on those bundle interfaces.</li> </ol>
CSCsz20671	<p>Symptoms: During PRE module switchover, each of the line cards unnecessarily updates the toaster information.</p> <p>Conditions: This issue is seen during a PRE switchover triggering the update.</p> <p>Workaround: There is no workaround.</p>
CSCsz21287	<p>Symptoms The following message is seen on execution of the test cable dcc cable command:</p> <pre>DCC abort! Target upstream is not associated with Cable</pre> <p>Conditions: This is seen on a Cisco uBR 10012 router running PRE1 processor module.</p> <p>Workaround: There is no workaround.</p>
CSCsz21661	<p>Symptom: The Gigabit Ethernet output for a 24-downstream wideband and narrowband SPA can get isolated from the port after repeated online insertion and removal (OIR) of the SPA within a short duration of time.</p> <p>Conditions: This issue is seen with repeated OIR of the SPA within a short duration of time and with repeated line protocol off/on within a short duration of time.</p> <p>Workaround: Reload the SPA using <b>hw-module bay reload</b> command.</p>

**Table 24** *Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsz22819	<p>Symptom: When using a wideband-SIP, the total count for the SPA in slot 1/1/0 is a sum of both SPAs, rather than the sum of itself. This can be using the show hw-module bay all counters rf-channel command.</p> <p>Conditions: This issue is seen in wideband-SIP when more than one SPAs are inserted in one SIP.</p> <p>Workaround: There is no workaround.</p>
CSCsz23805	<p>Symptoms: If a modular-cable channel with online modems is removed from its host and reconfigured to another host, the flows counter are incorrectly displayed.</p> <p>Conditions: This is seen when a modular-cable channel is removed from its host and reconfigured to another host.</p> <p>Workaround: There is no workaround.</p>
CSCsz27774	<p>Symptoms: The fiber node accepts non-existent upstream connectors, which may confuse the user on physical and logical topology.</p> <p>Conditions: This issue occurs when configuring non-existent upstream connectors on the fiber node.</p> <p>Workaround: Do not configure non-existent upstream connectors for the fiber node.</p>
CSCsz33086	<p>Symptoms: A channel enters the disabled state in a load balancing (LB) state machine.</p> <p>Conditions: This issue occurs if there is a channel whose condition is very bad, and is configured to a LB group with other channels. The state is set to disabled if it has too many LB failures on it. If this bad condition persists for a long time, and then it reverts, the LB state of this channel may get disabled.</p> <p>Workaround: Manually execute the clear cable load-balance state command.</p>
CSCsz34527	<p>Symptoms: After a cable line card switchover, the multicast traffic is forwarded by the CMTS but the traffic does not reach the customer premises equipment (CPE) behind the cable modem.</p> <p>Conditions: This issue is seen when a multicast QoS group is configured with encryption and there is a session using that QoS. This issue is seen after line card switchover for that multicast session.</p> <p>Workaround: Send an IGMP Leave from the CPE and then let the CPE join the session again.</p>
CSCsz42347	<p>Symptoms: The SPA BPI key index for a multicast Security Association Identifier (SAID) shows as zero after a PRE module or line card switchover. The index is displayed as Blaze_index in the <b>show interface cable &lt;x/y/z&gt; key sid</b> command.</p> <p>Conditions: This is seen after PRE module or line card switchover.</p> <p>Workaround: Remove the cable match command in the bundle interface and reset all the line cards that have multicast SAIDs with 0 SPA BPI index. If line card high availability is configured, keep the protect line card down.</p>

**Table 24** *Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsz44314	<p>Symptoms: Stale multicast BPI encryption keys remain on protect line cards that are in standby state.</p> <p>Conditions: This issue is seen while joining and leaving a multicast group (present in <b>cable match</b> command). Conduct a line card switchover from working to protect and then revert back to working from protect.</p> <p>Workaround: There is no workaround.</p>
CSCsz47949	<p>Symptom: The number of wideband modems collected via snmp walk and <b>show cable modem wideband</b> command does not match.</p> <p>Conditions: This is an intermittent problem and is not seen on all routers.</p> <p>Workaround: Use the <b>show cable modem wideband</b> command to have the exact number of wideband modems.</p>
CSCsz48159	<p>Symptom: The Cisco uBR10012 router with a PRE2 processor module configured for PacketCable Multimedia (PCMM) may crash with the following message in the log:</p> <pre>Invalid SID (1004) position for interface Cable6/0/4: CM 0015.a4f8.2076:Is used by CM &lt;mac&gt; SFID 17066 SID 120. SID container info: start 7933 end 7275 -Traceback= 608F7634 608F7D50 60221758 60221CC4 60222A48 6035198C 60302754 60303B98 603040C0 6034EACC 609F1870 609F185C</pre> <p>Conditions: The crash is observed on the Cisco uBR10012 router with a PRE2 processor module running Cisco IOS Release 12.2(33)SCB2 and with PCMM configured.</p> <p>Workaround: There is no workaround.</p>
CSCsz49641	<p>Symptom: The running configuration shows “-2147483” for <b>ip rsvp dsbm non-resv-send-limit [ burst   peak   rate ] 2147483</b> command, which may indicate that the CMs are not working properly.</p> <p>Conditions: This issue is seen while configuring the upper limit value for <b>ip rsvp dsbm non-resv-send-limit</b> command.</p> <p>Workaround: Do not configure upper limit value for <b>ip rsvp dsbm non-resv-send-limit</b> command.</p>
CSCsz50289	<p>Symptom: The cable linecard IPC timeouts and crashes.</p> <p>Conditions: This issue is seen on the cable linecard that may have a high CPU utilization.</p> <p>Workaround: There is no workaround.</p>
CSCsz52508	<p>Symptom: The <b>test cable dcc frequency</b> command to move one modem to target frequency does not work when the upstream channel id of the modem does not belong to the target downstream channel.</p> <p>Conditions: This issue only affect <b>test cable dcc frequency</b> command.</p> <p>Workaround: Use <b>test cable dcc frequency</b> command to move the modem where the upstream channel id belongs to the target downstream channel.</p>

**Table 24 Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)**

DDTS ID Number	Description
CSCsz52617	<p>Symptom: The cdxIfUpChannelAvgUtil reports incorrect numbers when rate adapt is enabled on router</p> <p>Conditions: This is seen when using SNMP to poll cdxIfUpChannelAvgUtil with rate adapt enabled.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1) Use CLI to obtain numbers</li> <li>2) Disable rate-adapt</li> </ol>
CSCsz61099	<p>Symptoms: A crash is observed when running the <b>show tech   redirect disk0:xxxx</b> command.</p> <p>Conditions: The following conditions may cause a crash:</p> <ul style="list-style-type: none"> <li>• Connecting to the CMTS using Secure Shell (SSH).</li> <li>• Executing the show tech   redirect disk command.</li> </ul> <p>Workaround: The crash does not occur with a Telnet session. If you use SSH to connect into the CMTS, do not redirect the output to DISK0 or DISK1.</p>
CSCsz67126	<p>Symptoms: Repeated PXF Crashes with the following error message are seen within the pxf crashinfo:</p> <pre>UBR10K Running PRE2 in 12.3(17b)BC9 or later may experience %PXF-2-FAULT: T0 HW Exception: CPU[t0r5c1] IWRA at 0x0D61 LR 0x0B40 %PXF-2-FAULT: T0 Exception summary: CPU[t0r5c1] Stat=0x00000006 HW=0x00100000 LB=0x00000000 SW=0x00000000</pre> <p>Conditions: This issue is seen on a Cisco uBR10012 router with PRE2 processor module and running Cisco IOS Release 12.3(17b)BC9 and later.</p> <p>Workaround: There is no workaround.</p>
CSCsz67488	<p>Symptom: The active time is inaccurate both downstream and upstream service flows with Cisco uBR10012 router The <b>show int cable x/y/c sid command</b> indicates a correct age value.</p> <p>Conditions: This issue was observed on both Cisco uBR7246VXR and Cisco uBR10012 routers running Cisco IOS Release 12.3(23)BC7 when DOCSIS QoS calls were created on a non DOCSIS QoS packetCable environment.</p> <p>Workaround: Use the <b>show interfaces cable x/yz sid</b> command to see the correct value.</p>
CSCsz78440	<p>Symptom: Modems based on Broadcom DPC3010 do not come wideband online.</p> <p>Conditions: This is seen on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC7 or earlier images.</p> <p>Workaround: There is no workaround.</p>

**Table 24** *Resolved Caveats in Cisco IOS Release 12.3(23)BC8 (continued)*

DDTS ID Number	Description
CSCsz82994	<p>Symptoms: When downstream load balancing (modem count method) is configured on a MAC Domain, where DOCSIS 3.0 and DOCSIS 2.0 are mixed, the total number of CMs to be load-balanced across the downstream interfaces are incorrect.</p> <p>Conditions: The wb_cm may be corrupted. The downstream interface may go into the initial state with active CMs.</p> <p>Workaround:Reload the CMTS.</p>
CSCsz83196	<p>Symptoms: The “No map buffer” error is seen during a PXF crash and modem drop offline.</p> <p>Workaround:There is no workaround.</p>
CSCta06866	<p>Symptom: When a modem is load balanced with Dynamic Channel Change (DCC), receives a “cdxCmtsCmOnOffNotification” OFF trap from the cmts, but no corresponding ON trap.</p> <p>Conditions: This is seen on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC2 with <b>snmp-server traps enable cable cm-onoff</b> command configured in the global configuration and <b>cable enable-trap [cm onoff-notification]</b> command on each interface along with load balancing</p> <p>Workaround: There is no workaround.</p>

## Open Caveats for Release 12.3(23)BC7

Table 25 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(23)BC7.

**Table 25** Open Caveats for Cisco IOS Release 12.3(23)BC7

DDTS ID Number	Description
CSCek29193	<p>Symptom: Swapping unlike MC520 line cards (s, u) causes modems to go offline, and configuration loss.</p> <p>Conditions: This issue occurs when the behavior of the cr10k card [slot/subslot] OIR-compatibility command is converted from default disabled to default enabled for all cable line cards.</p> <p>Workaround: Prior to exchanging line cards, configure OIR-compatibility for all slots.</p> <p>If the line card exchange occurs without configuring OIR-compatibility, and the problem has been discovered BEFORE a <b>wr mem</b> command is issued, perform the following procedure:</p> <ol style="list-style-type: none"> <li>1. Copy sec-nvram:startup-config to external box.</li> <li>2. Edit card types from MC520s-d to MC520u-d.</li> <li>3. Copy the modified file to nvram:startup-config, and also sec-nvram:startup-config</li> <li>4. Reload.</li> </ol> <p>This procedure is the only procedure which ensures that your frequency stacking and virtual interface configurations are preserved. Attempts to paste pieces of the previously stored running config will fail if frequency stacking or virtual interfaces are configured as the connectors must be un-assigned first.</p> <p>If a <b>wr-mem</b> has occurred, then the shutdown state, and blank config file for all interfaces will be written to both the primary and secondary nvram: as a result, the technique above will not work without resorting to an externally stored backup configuration for the system.</p>
CSCek41611	<p>Symptom: Cisco uBR10-MC5X20U cards may experience a silent reload.</p> <p>Conditions: This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>Workaround: Upgrade to Cisco IOS Release 12.2(33)SCB1.</p>
CSCsq64227	<p>Symptom: The number of downstream payload header suppression (PHS) rules for a cable MAC domain remains the same even though more downstreams can be added to the MAC domain (via Modular Downstreams).</p> <p>Workaround: There is no workaround.</p>
CSCsr59753	<p>Symptom: The Cisco IOS Release 12.3(23)BC2 mixed DOCSIS mode (atdma-tdma) achieves only 40 Unsolicited Grant Service (UGS) for an upstream whereas Cisco IOS Release 12.3(17b)BC9 achieves 48 UGS flows.</p> <p>Workaround: There is no workaround.</p>

Table 25 Open Caveats for Cisco IOS Release 12.3(23)BC7 (continued)

DDTS ID Number	Description
CSCsu33316	<p>Symptom: The cable line card (CLC) crashes after executing <b>clear arp</b> and <b>clear cable modem all delete</b> commands.</p> <p>Workaround: There is no workaround.</p>
CSCsu77588	<p>Symptom: Cable modems go offline with no alert or log message.</p> <p>Conditions: This occurs only on the Cisco uBR10-MC5X20U line cards on the Cisco uBR10012 router.</p> <p>Workaround: Use the <b>shutdown</b> and <b>no shutdown</b> commands on the affected interfaces or power cycle the cable line card.</p>
CSCsv12582	<p>Symptom: When running Cisco IOS Release 12.3(21a)BC7 or BC8, there are instances where the CPE device disappears from the cable host table and sometimes from the ARP table. In all cases, the CPE loses IP connectivity. This shows up across different CM vendors, different CLC types, different plants, and different Cisco uBR10012 routers. (This is also seen in earlier IOS versions, including 12.3(17b)BC8.)</p> <p>These are usually the symptoms seen:</p> <ul style="list-style-type: none"> <li>• The CPE loses connectivity.</li> <li>• The CPE does not show up on the CMTS when running any <b>show</b> commands.</li> <li>• Sometimes, the ARP entry for the CPE is seen in the ARP table.</li> <li>• When the CPE sends a DHCPDISCOVER packet, the CNR responds with DHCPOFFER. But for some reason, the CPE keeps sending DHCPDISCOVER.</li> <li>• After the <b>clear cable host</b> command is run a couple of times (until the error, “No such host” is seen), the CPE successfully acquires the IP address.</li> </ul> <p>Workaround: Run the <b>clear cable host</b> command for the CPE device until the device shows up in the CPE table again. This workaround does not work always.</p>
CSCsv14196	<p>Symptom: The secondary performance routing engine (PRE) crashes when the DBS function is applied to the wideband interface.</p> <p>Conditions: This occurs on a PRE2 running on Cisco IOS Release 12.3(23)BC2.</p> <p>Workaround: There is no workaround.</p>
CSCsv53276	<p>Symptom: The rf-channel 0 becomes unknown after hw-module reset.</p> <p>Workaround: Reload the router.</p>
CSCsv54656	<p>Symptom: The input rate counter of all Generic Route Encapsulation (GRE) tunnels is incorrect. It is doubled compared to the real value.</p> <p>Condition: This occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC1, 12.3(23)BC2, or 12.3(23)BC5.</p> <p>Workaround: There is no workaround.</p>

**Table 25** *Open Caveats for Cisco IOS Release 12.3(23)BC7 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsv59917	<p>Symptom: The Cisco Wideband SPA loses IP, MAC address, and RF channel configurations.</p> <p>Condition: This occurs if DOCSIS 3.0 configuration is not synchronized with the Cisco Wideband SPA after a Cisco IOS image upgrade.</p> <p>Workaround: Reload the Cisco uBR10012 router.</p>
CSCsv85159	<p>Symptom: The upstream ports configured as Hot Standby Connection-to-Connection Protocol (HCCP) protect show link down minor alarm when executing the <b>show facility-alarm status</b> command.</p> <p>Conditions: This occurs when the cable line card is configured as HCCP protect on a Cisco uBR10012 router running on Cisco IOS Release later than 12.3(23)BC2.</p> <p>Workaround: There is no workaround. This minor alarm does not affect the working of the system.</p>
CSCsv88650	<p>Symptom: Modems on modular interface take a long time to recovery or go offline after a switchover or revertback.</p> <p>Conditions: This occurs on active Cisco uBR10-MC5X20S and Cisco uBR10-MC5X20U line cards, modems on modular interface and mostly for Annex A modulation type.</p> <p>Workaround: There is no workaround.</p>
CSCsv94281	<p>Symptom: After the PRE switchover, the throughput of a multichannel or wideband interface is larger than the real value as per the <b>show interface</b> command. After 10 or 20 minutes, the throughput recovers automatically.</p> <p>Workaround: There is no workaround.</p>
CSCsw29191	<p>Symptom: When three-way calling (TWC), the admitted service flow of the side “on hold” still has traffic.</p> <p>Conditions: This occurs on a Cisco uBR10012 router running on Cisco IOS Release 12.3(23)BC and 12.2(33)SCB.</p> <p>Workaround: There is no workaround.</p>
CSCsw33866	<p>Symptom: Both the working and protect line cards are active.</p> <p>Conditions: This occurs when the suspend timer expires after a line card revertback immediately followed by a <b>no shutdown</b>.</p> <p>Workaround: Do not shutdown the active protect interface. Reset the protect card.</p>
CSCsw38849	<p>Symptom: The backup DOCSIS Timing and Control Card (DTCC) card experiences an unexpected reload.</p> <p>Conditions: This occurs on a backup DTCC on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC2.</p> <p>Workaround: There is no workaround.</p>
CSCsw68704	<p>Symptom: The wideband modem becomes wb-online.</p> <p>Conditions: This occurs when executing the <b>shutdown</b> and <b>no shutdown</b> commands on an active protect interface.</p> <p>Workaround: Do not shutdown an active protect interface.</p>

Table 25 Open Caveats for Cisco IOS Release 12.3(23)BC7 (continued)

DDTS ID Number	Description
CSCsw78391	<p>Symptom: Some downstream packets of Unsolicited Grant Service (UGS) traffic is dropped for 7 seconds when the cable modem sends a Dynamic Service Change (DSC) for the service flow.</p> <p>Conditions: This occurs when cable service flow activity-timeout is set to a value shorter than the call duration.</p> <p>Workaround: Set cable service flow activity-timeout value to be greater than the call duration time or use a different model of cable modem.</p>
CSCsw80300	<p>Symptom: The Committed Information Rate (CIR) value in <b>show hw-module bay all association wideband-channel</b> output changes to half after multiple switchover.</p> <p>Workaround: There is no workaround.</p>
CSCsw89288	<p>Symptom: Empty MAC address and IP address are displayed in the <b>show interface cable x/yz sid</b> command output.</p> <p>Conditions: This occurs on a Cisco uBR10012 router.</p> <p>Workaround: There is no workaround.</p>
CSCsw89385	<p>Symptom: The output of <b>show cable modem docsis version summary total</b> command is not displayed correctly.</p> <p>Conditions: This occurs on a Cisco uBR10012 router running on Cisco IOS Release 12.3(23)BC and 12.2(33)SCB with many cable modems.</p> <p>Workaround: There is no workaround.</p>
CSCsx32213	<p>Symptom: A Cisco router may reload reporting a bus error.</p> <p>Conditions: This has been observed on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC4.</p> <p>Workaround: There is no workaround.</p>
CSCsx45807	<p>Symptom: When the disk is full, data is sent to the route processor to be written to the disk continues to be written to the disk despite the disk being full.</p> <p>Conditions: This occurs when the IP Detail Record (IPDR) triggers high route processor CPU utilization when entries in the sflog table timeout, and the data is written to the disk.</p> <p>Workaround: Reduce the IPDR data collection interval.</p>
CSCsx48561	<p>Symptom: The Cisco Broadband Troubleshooter trace window shows incorrect data when triggering an upstream using the cable modem MAC address.</p> <p>Conditions: This occurs during upstream frequency stacking and with configurable MAC domains.</p> <p>Workaround: Remove frequency stacking and the configurable MAC domains.</p>
CSCsx52835	<p>Symptom: PXF crashes due to "DMA TBB Length Error".</p> <p>Workaround: There is no workaround.</p>
CSCsx53105	<p>Symptom: The Cisco uBR10012 router crashes for unknown reason.</p> <p>Workaround: There is no workaround.</p>

**Table 25** *Open Caveats for Cisco IOS Release 12.3(23)BC7 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsx57029	<p>Symptom: Incorrect MAC or IP address is displayed.</p> <p>Conditions: This occurs while executing <b>show cable mode [MAC   IP] access-group</b> command in Cisco uBR10012 running Cisco IOS Release 12.3(23)BC and Cisco IOS Release 12.2(33)SCB.</p> <p>Workaround: There is no workaround.</p>
CSCsx58392	<p>Symptom: Some Cisco uBR10012 routers respond incorrectly to tracert request of a Microsoft Windows PC.</p> <p>Workaround: There is no workaround.</p>
CSCsx62083	<p>Symptom: The standby performance routing engine (PRE) does not become active PRE after a PRE switchover.</p> <p>Conditions: This occurs when a PRE switchover happens while executing <b>show tech-support   redirect disk0: showtech</b> command.</p> <p>Workaround: Do not execute <b>show tech-support   redirect disk0: showtech</b> command while preparing for a PRE switchover.</p>
CSCsx67030	<p>Symptom: Spurious memory access traceback is seen while getting docsIfDownstreamChannelEntry.</p> <p>Conditions: This occurs when "broadband innovation" upconverter is used.</p> <p>Workaround: There is no workaround.</p>
CSCsx79753	<p>Symptom: The Cisco uBR10012 router reports MRI Unlink Error.</p> <p>Conditions: This occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(21a)BC6.</p> <p>Workaround: There is no workaround.</p>
CSCsx79870	<p>Symptom: Changing only the second choice channel width of an upstream configured with both the first and second choice channel width does not affect the configuration.</p> <p>Conditions: This occurs on a Cisco uBR10012 router running on Cisco IOS Release 12.3BC.</p> <p>Workaround: Modify the first choice channel width first and then modify or reconfigure the second choice.</p>
CSCsx95709	<p>Symptom: A booting secondary performance routing engine 2 (PRE2) crashes by configuring booted primary PRE2.</p> <p>Conditions: This occurs when the primary PRE2 is configured before the secondary PRE2 is up.</p> <p>Workaround: There is no workaround.</p>
CSCsy00714	<p>Symptom: The Cisco uBR10012 secondary performance routing engine (PRE) crashes due to an Error Interrupt.</p> <p>Conditions: This occurs on a Cisco uBR10012 router running on Cisco IOS Release 12.3(23)BC4 with redundant PREs.</p> <p>Workaround: There is no workaround.</p>

**Table 25**      **Open Caveats for Cisco IOS Release 12.3(23)BC7 (continued)**

DDTS ID Number	Description
CSCsy13775	<p>Symptom: Incorrect facility alarm description is displayed for some upstream ports.</p> <p>Conditions: This rare occurrence happens on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC5 and Cisco IOS Release 12.3(23)BC6. This occurs either after resetting a modular-host line card or reloading the Cisco uBR10012 router.</p> <p>Workaround: Use the <b>shutdown</b> and <b>no shutdown</b> commands on the upstream posts.</p>
CSCsy13870	<p>Symptom: The threshold for Cisco network registrar (CNR) and signal-to-noise ratio (SNR) for modulation profile 2 behaves incorrectly.</p> <p>Workaround: Configure both profile 1 and 2 by entering valid threshold values or use 0 to bypass.</p>
CSCsy13889	<p>Symptom: Minor alarms for all upstream ports appear after reloading the Cisco uBR10012 router when the cable interface is administratively shutdown.</p> <p>Conditions: This occurs while running Cisco IOS Release 12.3(17b)BC9, Cisco IOS Release 12.3(23)BC2, and Cisco IOS Release 12.3(23)BC6 on a Cisco uBR10012 router with the cable interface shutdown.</p> <p>Workaround: Use the <b>no shutdown</b> command and then shutdown the cable interface again.</p>
CSCsy16511	<p>Symptom: After a line card switchover, the modulation profile of the upstream is re-ordered.</p> <p>Workaround: Remove and re-apply the modulation profile configuration on the upstream after modifying the modulation profiles.</p>
CSCsy23311	<p>Symptom: The Cisco uBR10012 router crashes when upgrading from Cisco IOS Release 12.3(21a)BC6 to 12.3(23)BC6.</p> <p>Workaround: There is no workaround.</p>
CSCsy23745	<p>Symptom: The cable modems remain in online(pk) state.</p> <p>Conditions: This occurs on both the Cisco uBR10-MC5X20H and Cisco uBR10-MC5X20U cable line cards. This occurrence is limited to one cable line card and not the entire chassis.</p> <p>Workaround: Power cycle the cable line card.</p>

## Resolved Caveats for Release 12.3(23)BC7

Table 28 lists only severity 1 and 2 caveats and select severity 3 resolved caveats for Cisco IOS Release 12.3(23)BC7..

**Table 26** Closed Caveats for Cisco IOS Release 12.3(23)BC7

DDTS ID Number	Description
CSCei05676	<p>Symptom: The Gigabit Ethernet interface bounces when Cisco Discovery Protocol (CDP) is enabled.</p> <p>Conditions: This occurs when the CDP is enabled or disabled on an ESR-HH-1GE interface. This results in an interruption of traffic for 5 seconds.</p> <p>Workaround: There is no workaround.</p>
CSCsj10593	<p>Symptom: The TGW crashes.</p> <p>Conditions: This occurs on Cisco IOS Release 12.4(15.6) when the ISDN test call interface Serial1:23 22222 is issued at the Call Starter. This happens with Switch Types: OGW: primary-ni TGW: primary-dms100.</p> <p>Workaround: There is no workaround.</p>
CSCsk50429	<p>Symptom: Illegal access to a low address crashes the router.</p> <p>Conditions: This occurs on a Cisco router running Cisco IOS Release 12.3BC with OSPF.</p> <p>Workaround: There is no workaround.</p>
CSCsm55365	<p>Symptom: When configuring a new interface either cable or gigabit ethernet, some of the secondary IP addresses fail to install in the RIP database and as a result are not advertised by RIP.</p> <p>Conditions: This occurs on a Cisco uBR10000 router with a PRE2 running ubr10k2-k8p6u2-mz.123-17b.BC3 configured with secondary IP addresses and advertised major network under RIP v2.</p> <p>Workaround: Remove and reconfigure the secondary IP addresses under the interface and flap the interface.</p>
CSCso90058	<p>Symptom: The MSFC crashes with RedZone memory corruption.</p> <p>Conditions: This occurs while processing an Auto-RP packet with NAT enabled.</p> <p>Workaround: There is no workaround.</p>
CSCsr72301	<p>Symptom: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.</p> <p>The Cisco Security Response is posted at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http">http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http</a></p>
CSCsu48210	<p>Symptom: Packet cable calls fail. Delays are seen in the Get-Set-Ack response from the CMTS.</p> <p>Conditions: This occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC4 when SAMIS data is collected from the line cards.</p> <p>Workaround: Disable IPDR if possible and also reduce the amount of SNMP queries or polling.</p>

Table 26 Closed Caveats for Cisco IOS Release 12.3(23)BC7

DDTS ID Number	Description
CSCsu58139	Symptom: The <b>cable trust</b> command does not seem to have any impact on source verification Workaround: There is no workaround.
CSCsu96374	Symptom: Remote modems are using wrong indexes. Condition: This issue occurs on modems that are online from SPA downstream. When you run the <b>clear cable modem all reset</b> command, the modems come online from SPA downstream again. Workaround: To reset all the modems, use the <b>clear cable modem all delete</b> command.
CSCsv47575	Symptom: The Performance Routing Engine (PRE) crashes. Conditions: This happens when N+1 switchover occurs and the multicast quality of service (QOS) is configured on the Cisco uBR10012 router.
CSCsv52737	Symptom: The Cisco uBR10012 router does not properly re-initialize the sequence number field in the downstream extended header of the first packet transmitted on a newly created downstream ID. Workaround: There is no workaround.
CSCsv66509	Symptom: Bad dequeue error is seen at "CMTS METERING EXPORT Process". Conditions: This occurs when there are 45K cable modems configured with IP Detail Record (IPDR). Workaround: There is no workaround.
CSCsv73509	Symptom: tacacs/xtacacs is broken. Conditions: This occurs when <b>no aaa new-model</b> is configured and the authentication happens through the local when tacacs is configured. This happens for the exec users under vty configuration. Workaround: There is no workaround.
CSCsv83365	Symptom: The Performance Routing Engine2 (PRE2) may fail multiple times. Conditions: This issue occurs on the Cisco uBR10012 router with PRE2. Workaround: There is no workaround.
CSCsv85010	Symptom: MC520U card crashes due to Translation-Lookaside Buffer (TLB) BUS error when too many <b>cable modem xxxx change-frequency yyyy</b> commands are executed. Conditions: This issue occurs when multiple downstream (DS) ports are connected to one HFC. When one line card (LC) crashes, modems go online on the DS port of another LC using the load balancing feature. Workaround: There is no workaround.
CSCsw48049	Symptom: CMIpAddr returns 0 after line card switchover. Conditions: This occurs when IPDR and collector are configured. The collect gets cmipaddr = 0, it is different with "show cable modem" Workaround: There is no workaround.

**Table 26** *Closed Caveats for Cisco IOS Release 12.3(23)BC7*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsw52539	<p>Symptom: Cable metering collection enters “write-error” state and does not recover.</p> <p>Condition: This occurs when the cable metering is configured with default TCP parameters.</p> <p>Workaround: To prevent this issue, execute <b>ip tcp path-mtu-discovery</b> command. To clear the “hung” state and to allow the next iteration of cable metering to occur, use <b>test cable metering abort</b> command.</p>
CSCsw71440	<p>Symptom: The upstream bitmap is not updated after changing the max-ports.</p> <p>Conditions: This occurs when the upstream max-ports is changed using <b>cable upstream max-ports</b> command, and the upstream connector is configured to the new upstream channel.</p> <p>Workaround: Remove and reconfigure the cgd configuration under the MAC domain if the max-ports is changed.</p>
CSCsw78501	<p>Symptom: The Ingress Noise Cancellation functionality on the upstream is incorrectly activated or deactivated.</p> <p>Conditions: This occurs when an odd logical upstream channel ID is used with an even physical port ID and vice versa. This affects the Cisco uBR10-MC5X20H, and Cisco uBR10-MC2X8U line cards.</p> <p>Workaround: Use odd logical upstream channel ID with odd physical port ID and the even logical upstream channel ID with an even physical port ID.</p>
CSCsw79768	<p>Symptom: SNMP GetNext requests for docsQoSServiceFlowPrimary (also known as 1.3.6.1.2.1.10.127.7.1.3.1.8 or docsQoSServiceFlowEntry.8) are rejected. Still, if a certain docsQoSServiceFlowPrimary entry is polled with SNMP Get directly [after some additional calculations are performed to determine the index value], the value is returned as expected.</p> <p>Conditions: UBR7114E running 12.3(21a)BC3</p> <p>Workaround: Poll the individual values following the steps of the procedure suggested in SR 610144513</p>
CSCsw88346	<p>Symptom: The cable modems remain in init(i), init(o) after a TFTP server outage with Dynamic Shared Secret (DSS) on interfaces configured with DMIC Reject or Marked.</p> <p>Conditions: This occurs on both Cisco uBR7200 and Cisco uBR10012 routers running different Cisco IOS Releases 12.3(9a)BC6, 12.3(13a)BC1, and 12.3(23)BC2. This is seen only on the interfaces configured with DSS and when the TFTP server is not reachable.</p> <p>Workaround: Remove DSS from the cable interface.</p>
CSCsx07000	<p>Symptom: Some cable modems remain in the “sreject(na)” state.</p> <p>Conditions: This occurs when a cable modem returns “partial-service(30)” as confirmation-code in the REG-ACK message. DOCSIS3.0 defines partial-service as a successful confirmation-code but the cable modem does not proactively perform MAC reinitialization.</p> <p>Workaround: The cable modem must be reset manually.</p>

**Table 26**      **Closed Caveats for Cisco IOS Release 12.3(23)BC7**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsx10305	<p>Symptom: Removing the dot1q vc map causes WAN interface to flap.</p> <p>Conditions: This occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3BC. Removing the last dot1q vc map in the running configuration causes the WAN interface to flap.</p> <p>Workaround: There is no workaround.</p>
CSCsx24746	<p>Symptom: Per MAC domain statistics are not available.</p> <p>Workaround: Added a new command <b>show cable mac-domain cX/Y/Z forwarding</b> to show all the interfaces (wideband/modular) and statistics belonging to the MAC domain.</p>
CSCsx35612	<p>Symptom: Cable metering is stuck in "in progress" state and no collection data is transmitted.</p> <p>Conditions: This occurs on a Cisco uBR10012 router ESR-PRE2 running Cisco IOS Release 12.3(23)BC2 with cable metering.</p> <p>Workaround: Issue a "Test cable meter abort" to clear the problem and force Cable Meter process to restart.</p>
CSCsx37572	<p>Symptom: The initial term exec prompt timestamp state may not be retained.</p>
CSCsx41593	<p>Symptom: Secondary PRE keeps crashing due to bus error.</p> <p>Condition: This occurs after changing the bonding-group-id on the wideband interface and after PRE switchover, or hw-module sec-cpu reset.</p> <p>Workaround: Power off and on the chassis or reload on Active PRE.</p>
CSCsx57790	<p>Symptom: ccwbFiberNodeNBIfIndx returns 0 when the item's rfid belongs to modular interface.</p> <p>Conditions: This occurs when the fiber node is configured with downstream modular cable and then getmany -v2c ccwbFiberNodeNBIfIndx</p> <p>Workaround: There is no workaround.</p>
CSCsx58991	<p>Symptom: The protect line card is showed as revertive in <b>show hccp detail</b> command output even though <b>no member subslot x/y revertive</b> is configured.</p> <p>Conditions: This occurs after removing the working line card configuration and reconfiguring it.</p> <p>Workaround: Reconfigure using <b>no member subslot x/y revertive</b>.</p>
CSCsx62927	<p>Symptom: The IPDR data collection from the cable line card to the route processor congests the Backplane Ethernet (BPE) due to its high bursty traffic pattern.</p>
CSCsx64397	<p>Symptom: The L1 ISIS router does not install the default route to a L1L2 router in its routing table.</p> <p>Conditions: This occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3BC.</p> <p>Workaround: Use the <b>clear ip route *</b> or <b>clear isis *</b> command.</p>

**Table 26** *Closed Caveats for Cisco IOS Release 12.3(23)BC7*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsx65344	<p>Symptom: The w-online wide band modem provisioned with 2-channel bonding for high downstream rates are limited to 35Mbps downstream throughput.</p> <p>Conditions: This occurs on a Cisco uBR10012 router with PRE2 running Cisco IOS Release 12.3(23)BC4 with SIP and SPA wideband controllers in M-CMTS channel bonding setup.</p> <p>Workaround: Execute the <b>shutdown</b> and <b>no shutdown</b> commands on the corresponding wideband interface.</p>
CSCsx76442	<p>Symptom: After a Performance Routing Engine (PRE) failover, some modems and their CPEs are not reachable by IP.</p> <p>Conditions: This issue occurs on the Cisco uBR10012 router with ESR-PRE2.</p> <p>Workaround: Failover back to the original PRE or use the <b>clear cable modem</b> command to delete the affected modem.</p>
CSCsx77978	<p>Symptom: The downstream load is not balanced when the downstream load balance group is configured with us-across-ds policy.</p> <p>Workaround: Do not configure us-across-ds policy on the downstream load balance group.</p>
CSCsx79863	<p>Symptom: The channel utilization percentage calculated is inaccurate.</p> <p>Conditions: This occurs when “rate-adapt” is configured for an upstream channel and under certain configurable conditions, the MAC scheduler for that upstream allocates additional data grants to one or more cable modems in a given MAP message. When the data grants are not used by the cable modem(s), the utilization calculation by the scheduler are skewed.</p> <p>Workaround: There is no workaround.</p>
CSCsx81399	<p>Symptom: The LED on the HCCP protected downstream port illuminates when the protected downstream port is in standby mode.</p> <p>Conditions: This occurs on Cisco uBR10012 router with HCCP running Cisco IOS Release 12.3(23)BC2, 12.3(23)BC5, and 12.3(23)BC6.</p> <p>Workaround: There is no workaround.</p>
CSCsx96155	<p>Symptom: After changing the load-interval on the route processor, the interface load-interval on the line card does not change.</p> <p>Workaround: There is no workaround.</p>
CSCsy05419	<p>Symptom: An error message is not displayed when the terminal monitor is disabled.</p> <p>Conditions: This occurs when the upstream is configured for three step dynamic modulation and is added to a spectrum group.</p> <p>Workaround: There is no workaround.</p>
CSCsy12888	<p>Symptom: The Internet Control Message Protocol (ICMP) IP address is displayed as 0 in <b>show pxf cpu subblock bundle</b> command.</p> <p>Workaround: There is no workaround.</p>

**Table 26** *Closed Caveats for Cisco IOS Release 12.3(23)BC7*

DDTS ID Number	Description
CSCsy28104	<p>Symptom: The cable modems fail to go online(pt) with KEK authentication rejection.</p> <p>Conditions: This occurs from Cisco IOS Release 12.3(21)BC.</p> <p>Workaround: Provision the modems to sign on using DOCSIS 1.0 configuration files. But it is suggested to upgrade or replace these modems.</p>
CSCsy40915	<p>Symptom: The SNMP service primary flow counters include the pre-registration statistics while the corresponding CLI counters do not. The ARP packets from the CMTS are not mapped to the MAC destination address based on the MAC classifiers.</p> <p>Conditions: This occurs on both the upstream and downstream on the Cisco uBR7200 router and on the upstream on the Cisco uBR10012 router.</p> <p>Workaround: There is no workaround.</p>
CSCsy48072	<p>Symptom: The SPA interface goes down.</p> <p>Conditions: This occurs with SPA-24XDS-SFP on a Cisco uBR10012 router with PRE2 running Cisco IOS Release 12.3(23)BC6.</p> <p>Workaround: Execute <b>hw-module subslot 1/0 reset</b> command to recover the interfaces.</p>

## Open Caveats for Release 12.3(23)BC6

Table 27 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(23)BC6.

**Table 27** *Open Caveats for Cisco IOS Release 12.3(23)BC6*

DDTS ID Number	Description
CSCsw43954	<p>Symptom: Active Performance Routing Engine2 (PRE2) crashes in uBR10012 router due to IP-ARP related issues.</p> <p>Workaround: There is no workaround.</p>
CSCsv85010	<p>Symptom: MC520U card crashes due to Translation-Lookaside Buffer (TLB) BUS error when too many <b>cable modem xxxx change-frequency yyyy</b> commands are executed.</p> <p>Conditions: This issue occurs when multiple downstream (DS) ports are connected to one HFC. When one line card (LC) crashes, modems go online on the DS port of another LC using the load balancing feature.</p> <p>Workaround: There is no workaround.</p>
CSCsw20867	<p>Symptom: The Gigabit Ethernet interface is getting reset after configuring <b>no cdp enable</b> command.'</p> <p>Conditions: This issue occurs when the interface is running and cdp is enabled.</p> <p>Workaround: There is no workaround.</p>

**Table 27** *Open Caveats for Cisco IOS Release 12.3(23)BC6 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsw49188	<p>Symptom: Cable metering fails and enters a 'hung' state.</p> <p>Condition: This issue is observed when the <b>ip tcp timestamp</b> command is configured globally.</p> <p>Workaround: Do not use the <b>ip tcp timestamp</b> command.</p>
CSCsv83365	<p>Symptom: The Performance Routing Engine2 (PRE2) may fail multiple times.</p> <p>Conditions: This issue occurs on the Cisco uBR10012 router with PRE2.</p> <p>Workaround: There is no workaround.</p>
CSCsv52737	<p>Symptom: The Cisco uBR10012 router does not properly re-initialize the sequence number field in the downstream extended header of the first packet transmitted on a newly created downstream ID.</p> <p>Workaround: There is no workaround.</p>
CSCsu96374	<p>Symptom: Remote modems are using wrong indexes.</p> <p>Condition: This issue occurs on modems that are online from SPA downstream. When you run the <b>clear cable modem all reset</b> command, the modems come online from SPA downstream again.</p> <p>Workaround: To reset all the modems, use the <b>clear cable modem all delete</b> command.</p>
CSCso59575	<p>Symptom: The Cable Modem Termination System (CMTS) is truncating the RF Switch names to 30 characters (the maximum length permitted for an RF Switch name) instead of displaying error messages for crossing the maximum limit.</p> <p>Conditions: This issue occurs when more than 30 characters are entered for the RF Switch name.</p> <p>Workaround: There is no workaround.</p>
CSCsm00986	<p>Symptom: Traceback occurs when the Hot Standby Connection-to-Connection Protocol (HCCP) member is removed through the console and when the <b>show hccp channel-switch</b> command is run from the VTY session almost simultaneously.</p> <p>Workaround: There is no workaround.</p>
CSCsw35379	<p>Symptom: Periodic 1-second delays between the CMTS transmission of SAMIS packets; enough of these are occurring to make a significant impact on overall SAMIS transfer time.</p> <p>Workaround: There is no workaround.</p>
CSCsw51992	<p>Symptom: Invalid/corrupt values seen for OctetsPassed and PacketsPassed fields in SAMIS records.</p> <p>Conditions: CMTS with wideband SPA configured, query the service flow counters using SAMIS, snmp or show CLI, sometimes it will show wrong value for the octets or/and packets for the wideband modems or narrowband modems but using the remote SPA channel as primary downstream.</p> <p>Workarond: There is no workaround.</p>

Table 27 Open Caveats for Cisco IOS Release 12.3(23)BC6 (continued)

DDTS ID Number	Description
CSCsl35163	<p>Symptom: The range-backoff configuration value changes from “range-backoff 3 6” to “range-backoff automatic” for upstream in a frequency stacking scenario.</p> <p>Condition: This change is noticed after the following commands are executed to un-configure and re-configure the cable interface:</p> <ol style="list-style-type: none"> <li><b>cable upstream max-ports 6</b></li> <li><b>no cable upstream max-ports</b></li> <li><b>cable upstream max-ports 6</b></li> </ol> <p>Workaround: Modify the <i>range_backoff</i> value in the <i>cmts_mac_hwsb_us_init</i> file according to the line card type.</p>
CSCsv12582	<p>Symptom: When running Cisco IOS Release 12.3(21a)BC7 or BC8, there are instances where the CPE device disappears from the cable host table and sometimes from the ARP table. In all cases, the CPE loses IP connectivity. This shows up across different CM vendors, different CLC types, different plants, and different Cisco uBR10012 routers. (This is also seen in earlier IOS versions, including 12.3(17b)BC8.)</p> <p>These are usually the symptoms seen:</p> <ul style="list-style-type: none"> <li>The CPE loses connectivity.</li> <li>The CPE does not show up on the CMTS when running any <b>show</b> commands.</li> <li>Sometimes, the ARP entry for the CPE is seen in the ARP table.</li> <li>When the CPE sends a DHCPDISCOVER packet, the CNR responds with DHCP OFFER. But for some reason, the CPE keeps sending DHCPDISCOVER.</li> <li>After the <b>clear cable host</b> command is run a couple of times (until the error, “No such host” is seen), the CPE successfully acquires the IP address.</li> </ul> <p>Workaround: Run the <b>clear cable host</b> command for the CPE device until the device shows up in the CPE table again. This workaround does not work always.</p>
CSCsr59753	<p>Symptom: In certain Cisco IOS releases, mixed docsis mode (atdma-tdma) can only achieve 40 UGS for an upstream.</p> <p>Condition: This may be the result of mixed mode and modems.</p> <p>Workaround: There is no workaround.</p>
CSCsu58139	<p>Symptom: The <b>cable trust</b> command does not seem to have any impact on source verification</p> <p>Workaround: There is no workaround.</p>
CSCsv59917	<p>Symptom: The Cisco Wideband SPA loses IP, MAC address, and RF channel configurations.</p> <p>Condition: This occurs if DOCSIS 3.0 configuration is not synchronized with the Cisco Wideband SPA after a Cisco IOS image upgrade.</p> <p>Workaround: Reload the Cisco uBR10012 router.</p>

**Table 27** *Open Caveats for Cisco IOS Release 12.3(23)BC6 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsu01822	<p>Symptom: The CMTS crashes at c10k_remote_crash_interrupt.</p> <p>Condition: This issue occurs with continuous 21BC customer configurations.</p> <p>Workaround: There is no workaround.</p>
CSCsv54656	<p>Symptom: The input rate counter of all Generic Route Encapsulation (GRE) tunnels is incorrect. It is doubled compared to the real value.</p> <p>Condition: This occurs on a Cisco uBR10012 router running Cisco IOS 12.3(23)BC1, 12.3(23)BC2, or 12.3(23)BC5.</p> <p>Workaround: There is no workaround.</p>
CSCsw43250	<p>Symptom: The CMTS crashes when the policy map is removed.</p> <p>Workaround: Do not remove the policy map.</p>
CSCsv60404	<p>Symptom: A cable modem's throughput is reduced from 30 Mbps to 24 Mbps by starting a single Unsolicited Grant Service (UGS) voice flow on another cable modem. Once the voice flow is stopped, the modem's throughput returns to 30 Mbps.</p> <p>Workaround: There is no workaround.</p>
CSCso60646	<p>Symptom: When the last RF channel is removed from a wideband cable interface, the interface's bandwidth is not reset to zero as per the <b>show interface wideband-cable downstream</b> command.</p> <p>Workaround: There is no workaround.</p>
CSCsr43079	<p>Symptom: When the standby PRE is reloaded, the current STM monitoring details are not displayed correctly in the output of the <b>show cable qos enforce-rule verbose</b> command.</p> <p>Condition: This occurs if the standby PRE is reloaded when the active PRE is up. This does not occur if the standby PRE is not reloaded. This issue does not affect STM functionality. The standby PRE will get the correct monitoring details in the next monitoring period.</p> <p>Workaround: There is no workaround.</p>
CSCsq01701	<p>Symptom: Resetting the wideband cable modems make them come w-online and the upstream STM enforce- rule configuration does not shape their traffic as expected.</p> <p>Condition: This issue can be seen if modems are in penalty state and for some reason get reset at that time. Normally modems in penalty state do not get reset. If they get reset, they will come online and not shape the traffic only for that penalty.</p> <p>Workaround: There is no workaround.</p>
CSCso57024	<p>Symptom: The Cisco vendor-specific 'Wideband Channel ID' option (vendor-specific option 14) does not work.</p> <p>Condition: This issue is observed when using a recent version of Scientific Atlanta wideband DPC2505 modem with the Cisco uBR10012 router.</p> <p>Workaround: There is no workaround.</p>

**Table 27**      **Open Caveats for Cisco IOS Release 12.3(23)BC6 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsw14622	Symptom: For deleted service flows the last character in the Service Class Name field is dropped in SAMIS records as well as in the SNMP MIB docsQosServiceFlowLogServiceClassName
CSCsw52539	Symptom: Cable metering collection enters 'write-error' state and doesn't recover. Condition: Cable metering configured with default TCP parameters. Workaround: Run the <b>ip tcp path-mtu-discovery</b> command to help prevent occurrences of the issue. Run the <b>test cable metering abort</b> command to clear the 'hung' state and to allow the next iteration of cable metering to occur.

**Table 27**      **Open Caveats for Cisco IOS Release 12.3(23)BC6 (continued)**

DDTS ID Number	Description
CSCsv60054	<p>Symptom : The CMTSdownIfName reported by SAMIS is always Cable x/x/x-downstream for all downstream service flows despite the service flow belonging to the Wideband-Cable x/x/x:x or the Modular-Cable x/x/x:x type downstreams bonding group.</p> <p>Condition : This occurs for regular flows on the modular-cable downstreams and for flows on a bonding group.</p> <p>Workaround : There is no workaround.</p>
CSCsw64086	<p>Symptom: Cable modems may get stuck in 'expired' state with low signal-to-noise ratio (SNR) when the pre-equalization feature is enabled.</p> <p>Condition: This issue is observed on on a Cisco uBR10012 router with PRE2 and the uBR10-MC5x20U and uBR10-MC5x20S line cards.</p> <p>Workaround:</p> <p>Use the following modulation profile for the 64 QAM.</p> <pre> cab modulation-prof 224 request 0 16 0 48 qpsk scram 152 no-diff 32 fixed qpsk0 1 2048 cab modulation-prof 224 initial 5 34 0 48 16qam scram 152 no-diff 384 fixed qpsk1 1 2048 cab modulation-prof 224 station 5 34 0 48 16qam scram 152 no-diff 384 fixed qpsk1 1 2048 cab modulation-prof 224 a-short 6 76 3 22 64qam scram 152 no-diff 64 short qpsk1 1 2048 cab modulation-prof 224 a-long 9 232 0 22 64qam scram 152 no-diff 64 short qpsk1 1 2048 cab modulation-prof 224 a-ugs 9 232 0 22 64qam scram 152 no-diff 64 short qpsk1 1 2048 </pre> <p>For a robust VoIP:</p> <pre> cab modulation-prof 224 a-ugs 9 232 0 22 16qam scram 152 no-diff 64 short qpsk1 1 2048 </pre> <p>Use the following modulation profile for the 16 QAM:</p> <pre> cab modulation-prof 223 request 0 16 0 44 qpsk scram 152 no-diff 32 fixed qpsk0 1 2048 cab modulation-prof 223 initial 5 34 0 48 16qam scram 152 no-diff 384 fixed qpsk1 1 2048 cab modulation-prof 223 station 5 34 0 48 16qam scram 152 no-diff 384 fixed qpsk1 1 2048 cab modulation-prof 223 a-short 6 76 7 22 16qam scram 152 no-diff 64 short qpsk1 1 2048 cab modulation-prof 223 a-long 9 232 0 22 16qam scram 152 no-diff 64 short qpsk1 1 2048 cab modulation-prof 223 a-ugs 9 232 0 22 16qam scram 152 no-diff 64 short qpsk1 1 2048 </pre>

## Resolved Caveats for Release 12.3(23)BC6

Table 28 lists only severity 1 and 2 caveats and select severity 3 resolved caveats for Cisco IOS Release 12.3(23)BC6.

**Table 28** Resolved Caveats for Cisco IOS Release 12.3(23)BC6

DDTS ID Number	Description
CSCsm27071	<p>A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:</p> <ul style="list-style-type: none"> <li>• The configured feature may stop accepting new connections or sessions.</li> <li>• The memory of the device may be consumed.</li> <li>• The device may experience prolonged high CPU utilization.</li> <li>• The device may reload. Cisco has released free software updates that address this vulnerability.</li> </ul> <p>Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip</a></p>
CSCsv04836	<p>Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.</p> <p>In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.</p> <p>Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24</a></p>
CSCsv52737	<p>Symptom: The Cisco uBR10012 router does not properly re-initialize the sequence number field in the DS extended header of the first packet transmitted on a newly created downstream ID.</p> <p>Workaround: There is no workaround.</p>

**Table 28 Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)**

DDTS ID Number	Description
CSCsk64158	<p>Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp</a></p>
CSCsw24700	<p>Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:</p> <p>Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.</p> <p>SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.</p> <p>Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link:  <a href="http://www.cisco.com/en/US/products/csa/cisco-sa-20090325-webvpn.html">http://www.cisco.com/en/US/products/csa/cisco-sa-20090325-webvpn.html</a></p>
CSCsg00102	<p>Symptoms: SSLVPN service stops accepting any new SSLVPN connections.</p> <p>Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.</p>
CSCso04657	<p>Symptoms: SSLVPN service stops accepting any new SSLVPN connections.</p> <p>Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.</p>
CSCsv98326	<p>Symptom: ifStackStatus corruption occurs while configuring the wideband interface after inserting new jacket and shared port adapter (SPA) card.</p> <p>Workaround: Reload the Cable Modem Termination System (CMTS).</p>
CSCsu63999	<p>Symptom: The spectrum group is not assigned to the line card (LC) after adding ~4093 Transparent LAN Service (TLS) configuration lines and reloading the LC through 'hw-module reset' command. Similarly, modems are missing for the LC and upstreams are disabled.</p> <p>Workaround: There is no workaround.</p>

Table 28 Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)

DDTS ID Number	Description
CSCsu44606	<p>Symptom: Duplicate traps are generated when configuring SNMP traps for cable billing operations.</p> <p>Workaround: There is no workaround.</p>
CSCsr54283	<p>Symptom: When the active DTI is reset, SNMP traps are not generated.</p> <p>Workaround: Enable the following commands so that Syslog forwards the traps to SNMP:</p> <pre>snmp-server enable traps syslog snmp-server enable traps fru-ctrl</pre> <p style="text-align: center;"></p> <p><b>Caution</b> Enabling the above commands may overload the Network Management System (NMS) in the network.</p>
CSCsv71096	<p>Symptom: After moving the 2 Gigabit Ethernet modules from slot 1 and 2 to slot 3 and 4 in the Cisco uBR10012 router, the interface is not providing SNMP information for utilizing graphing on the card in slot 3. The issue persists in slot 3 even after performing a shut and no shut, and Online Insertion and Removal (OIR).</p> <p>Workaround: There is no workaround.</p>
CSCsr74835	<p>Symptom: There may be an overflow of destination buffer due to unspecified bounding length.</p> <p>Workaround: There is no workaround.</p>
CSCsu97227	<p>Symptom: An incorrect value (instead of the actual value BW 37500 Kbit) is displayed when <b>show interface Cable slot/subslot/port</b> command is used in a cable interface configured with 256QAM Downstream Modulation. Service degradation is also experienced during this behavior.</p> <p>Workaround: Move the modulation from 256QAM to 64QAM and back.</p>
CSCsv29206	<p>Symptom: The <b>show interface slot/subslot/port modem 0</b> command displays duplicate MAC entries.</p> <p>Workaround: There is no workaround.</p>
CSCsv65320	<p>Symptom: A spurious memory traceback is observed on the uBR10000 series line card after boot up.</p> <p>Condition: This issue occurs when CLC queries the docsIfUpstreamChannelTable while coming up.</p> <p>Workaround: There is no workaround.</p>

**Table 28** *Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsv30681	<p>Symptom: Modems capable of bonding fails to get online when the following configuration line is present: 'cable service attribute ds-bonded downstream-type bonding-enabled [enforce]'</p> <p>Conditions: When the above configuration line is present, the Cable Modem Termination System (CMTS) attempts to move modems capable of bonding to primary channels that are capable of bonding through a downstream frequency override (DFO) during initial ranging. However, if the target frequency is impaired, the cable modem (CM) fails to successfully initialize on that frequency. When the CM returns to the bonding downstream channel, it will once again receive a DFO to the bonding capable downstream. If all bonding capable downstream channels are impaired, the CM will not come online.</p> <p>Workaround: There is no workaround.</p>
CSCsv05377	<p>Symptom: Adding a new cable bundle sub-interface with ip address deletes all the Customer Premises Equipments (CPEs) or Hosts or multimedia terminal adapters (MTAs) behind the cable modem on existing cable bundle sub-interface. It also breaks the IP connectivity from Cable Modem Termination System (CMTS) to the CPEs or Hosts or MTAs as they are deleted from the CPE table. The same issue occurs when a newly created cable bundle sub-interface is deleted.</p> <p>Workaround: There is no workaround.</p>
CSCsv30617	<p>Symptom: When the IP Set-top-box (STB) or Customer Premises Equipment (CPE) sends an IGMPv2 leave for a multicast group that is configured for static forwarding based on "ip igmp static-group" interface configuration on the Cable Modem Termination System (CMTS), then the CMTS stops forwarding the stream.</p> <p>Conditions: This issue happens when there is a static-group configuration for Source Specific Multicast (SSM) on the CMTS and CPE is sending Advanced Services Module (ASM) join to that SSM group range. When Internet Group Management Protocol (IGMP) leave for that SSM range is received, the CMTS mistakenly removes the forwarding entries and the multicast forwarding stops.</p> <p>Workaround: Add an input Access Control List (ACL) to the bundle interface to block all IGMP packets on the upstream for streams that are configured for static forwarding on the CMTS.</p>
CSCsw25116	<p>Symptom: Cable TLS (Transparent Lan Service) data traffic either stops or gets forwarded as unencrypted following an Online Insertion and Removal (OIR) of the cable line card.</p> <p>Conditions: This issue occurs when the Modular Cable primary downstream and the Modular host are on a different line card than the MAC-domain host interface of the CM configured for TLS service.</p> <p>Workaround: There is no workaround.</p>
CSCsu95787	<p>Symptom: When traffic is sent to a shared port adapters (SPA) bay without any SPA, the packets get accumulated on the SPA carrier card causing link level flow control to the Parallel Express Forwarding (PXF) data path. As a result, traffic to the peer SPA gets dropped and the modems are going offline.</p> <p>Workaround: Reload the SPA carrier card.</p>

Table 28 Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)

DDTS ID Number	Description
CSCsu58767	<p>Symptom: Modems registered on remote modular interface are going offline during line card revertback when "cable default-phy-size" or "cables upstream x ingress cancellation" is not having the same value as default value.</p> <p>Workaround: Use 'default cable default-phy-size' or 'default cable upstream x ingress-noise-cancellation' on the interface.</p>
CSCsv48215	<p>Symptom: The association information between a Wideband interface and a MAC domain interface on the active working LC is not getting updated correctly on the standby Performance Routing Engine (PRE) after an N+1 revert to the working LC.</p> <p>When the standby PRE becomes active, changes are not updated correctly on the associated interface, for example, a configuration change to the downstream channel-id on the Wideband interface will not be updated on the MAC domain interface and vice-versa.</p> <p>Workaround: There is no workaround.</p>
CSCsv38530	<p>Symptom: The standby PRE crashes after bootup with the following error:</p> <pre>%UBR10K_REDUNDANCY-4-RP_HA_STDBY_INCONSISTENT: Standby PRE dropping inconsistent sync messages.</pre> <p>Condition: This occurs if you use the <b>shut</b> command to shut down the standby working interface.</p> <p>Workaround: Do not shut down the standby working interface.</p>
CSCsw47192	<p>Symptom: The active PRE2 crashes when the rf-switch snmp community string is removed.</p> <p>Condition: This occurs on a Cisco uBR10012 router when the rf-switch snmp community string is removed after removing all line cards from the redundancy group.</p> <p>Workaround: There is no workaround.</p>
CSCsm87471	<p>Symptom: The Cisco uBR10-MC5X20H line card crashes resulting in a breakpoint exception.</p> <p>The following error message is reported in the crashinfo file:</p> <pre>cr10k_clc_pre_poll: IPC not up. Reloading Line Card..</pre> <p>Condition: This is observed on a Cisco uBR10012 router running Cisco IOS Release 12.3(21a)BCx or 12.3(23)BC.</p> <p>Workaround: There is no workaround.</p>
CSCsw24218	<p>Symptom: The Cisco uBR10-MC5X20H line card or RP might fail if you run the <b>test cable phydump</b> command continuously.</p> <p>Condition: This occurs if you run the <b>test cable phydump</b> command continuously from the RP. This might also cause line card CPUHOG, IPC time-out, and line card crash or reset.</p> <p>Workaround: Use the <b>sleep</b> command to delay the action in seconds.</p>

**Table 28 Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsv06998	<p>Symptom: Sometimes the HCCP function takes longer time to enter into the “ready” state. It means when you run the <b>show hccp brief</b> command the “WaitToResync” timer does not stop. You need to wait for several seconds.</p> <p>Condition: This is observed on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC5 only.</p> <p>Workaround: There is no workaround.</p>
CSCsu50644	<p>Symptom: The standby line card may crash after a line card switchover.</p> <p>This is observed on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC.</p> <p>Workaround: There is no workaround.</p> <p>Modems will remain online without any data loss even if the standby line card crashes.</p>
CSCsu52820	<p>Symptom: All cable modems on the remote downstream channel go offline and can not become online again.</p> <p>Condition: This occurs with the following two conditions:</p> <ul style="list-style-type: none"> <li>• If the protect card is active, and a PRE switchover takes place.</li> <li>• If the working card’s slot/subslot combination is less than the protect card’s combination. For example, configure 5/0 as a working card and 5/1 as a protect card.</li> </ul> <p>Workaround: Reconfigure Channel Grouping Domain (CGD).</p>
CSCsv06559	<p>Symptom: Global HCCP configuration is broken after a line card is reset.</p> <p>Condition: Instead of protecting a single active line card, the protect card protects two active cards after global HCCP configuration.</p> <p>Workaround: Reset the protect card and one of the active cards.</p>
CSCsu36225	<p>Symptom: Two upstream ports on the same PHY receiver of a Cisco uBR10-MC5X20H line card show signal-to-noise ratio (SNR) degradation of about 10 dB.</p> <p>Condition: This occurs due to ingress-noise cancellation.</p> <p>Workaround: There is no workaround.</p>
CSCsv10205	<p>Symptom: Modems go offline.</p> <p>Condition: Modems go offline when Pre-Equalization (PRE-EQ) is enabled with ATDMA 64QAM 6.4Mz on an upstream port on a Cisco uBR10-MC5X20S line card.</p> <p>Workaround: Use a different modulation profile.</p>
CSCsv18798	<p>Symptom: Changing the frequency stacking configuration causes the upstream minislot sizes to differ from running configuration.</p> <p>Condition: When enabling or disabling the frequency stacking configuration, the upstream minislot sizes revert to system defaults based on the upstream DOCSIS mode.</p> <p>Workaround: Reload the line card or chassis.</p>

**Table 28 Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)**

DDTS ID Number	Description
CSCsv76612	<p>Symptom: An active PRE failover occurs and a crash info file is generated.</p> <p>Workaround: There is no workaround.</p>
CSCsv94281	<p>Symptom: After the PRE switchover, the throughput of a multichannel or wideband interface is larger than the real value as per the <b>show interface</b> command. After 10 or 20 minutes, the throughput recovers automatically.</p> <p>Workaround: There is no workaround.</p>
CSCso96838	<p>Symptom: Secondary PRE2 crashes.</p> <p>Condition: This issue is observed when the following exceptions are run:</p> <ul style="list-style-type: none"> <li>• no exception-slave core-file ubr3</li> <li>• no exception-slave dump 172.18.98.28</li> <li>• no exception core-file ubr3, and</li> <li>• no exception dump 172.18.98.28.</li> </ul> <p>Workaround: Do not remove the exception.</p>
CSCsw23217	<p>Symptom: The reset functionality for the Cisco uBR10-MC5X20H line card is broken.</p> <p>Condition: This occurs when the line card is reset after a failure and causes the following:</p> <ul style="list-style-type: none"> <li>• In most cases, the reset operation fails.</li> <li>• In some rare cases, one slot can not be booted up or wrong slots are reset.</li> </ul> <p>Workaround: There is no workaround.</p>
CSCsv29600	<p>Symptom: If the modular interface is deleted from legacy interface, trace back "Ib: Mo1/0/0:2:handle_stats_report_common(): no stats data" will show up and modem from the other line card could wait to come online on that interface.</p> <p>Condition: CMTS has configured modular cable interface with load balance group, and this load balance group includes interface from other line card.</p> <p>Workaround: Modular interfaces are not included in the load balance group that has interfaces from other line cards.</p>
CSCsv04307	<p>Symptom: DOCSIS 3.0 modems are not counted in the load balancing algorithm, but after line card switchover, the original D3.0 w-online modems are counted in, and the service flow counter is incorrect.</p> <p>Condition: This issue is observed during the start of the line card switchover.</p> <p>Workaround: There is no workaround.</p>
CSCsv00851	<p>Symptom: The <b>show cable load internal</b> command will report unknown interface or report the same interface twice.</p> <p>Conditions: This issue may be observed when configuring the modular-cable interface to the host interface.</p> <p>Workaround: Do not use the modular-cable interface.</p>

**Table 28**      **Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)**

DDTS ID Number	Description
CSCsw28992	<p>Symptom: Using the <b>test cable dcc</b> command from the modular to the native interface, the cable modem works fine. Using the <b>test cable dcc</b> command from the native to the modular drives the CM offline, at which point it is reported [offline] on another native downstream where it can never possibly register by the cable plant design. Finally the cable modem goes online on the right DS again.</p> <p>Condition: Wideband Cable deployment. The CM must fail to move from the native to the modular DS.</p> <p>Workaround: When the CM is allowed to recover it is reported under a correct interface.</p>
CSCsw47620	<p>Symptom: The <b>show controller modular-cable</b> command output displays incorrect temperature interrupt counts even while the wideband CMTS DOCSIS SPA temperature is normal.</p> <p>Condition: This issue is observed during normal SPA operating conditions.</p> <p>Workaround: There is no workaround.</p>
CSCsv62673	<p>Symptom: SPA crashes if log clear is executed while log dump has not finished its output.</p> <p>Conditions: This issue is observed under the following conditions.</p> <ol style="list-style-type: none"> <li>1. if-console x/y</li> <li>2. log dump</li> <li>3. log clear</li> <li>4. SPA is OIR / crashes but there is no crashinfo is logged</li> </ol> <p>Workaround: Always make sure that log dump is completed before clearing the log buffer.</p>
CSCsv63086	<p>Symptom: The Blaze Index value is not cleared from the Service flow when the wideband interface is shut down.</p> <p>Condition: This symptom is observed when the cable modem is in the w-online state. When the wideband interface is shut, WCM is offline. When the modem comes online, it uses the original Blaze Index.</p> <p>Workaround: There is no workaround.</p>
CSCsv91309	<p>Symptom: Wideband modems lose IP access after moving via DCC.</p> <p>Condition: This issue is observed on on a DOCSIS 3.0 cable modem running Cisco IOS 12.3(23)BC5 with Load Balance enabled or Test DCC command with init tech 1-4.</p> <p>Workaround: There is no workaround.</p>

**Table 28 Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)**

DDTS ID Number	Description
CSCsv91271	<p>Symptom: The <b>show cable modem</b> command displays the "Warning: Zero Blaze index for SFID" message after the wideband cable modem doing DCC.</p> <p>Conditions: This issue is observed under the following conditions.</p> <ul style="list-style-type: none"> <li>• Wideband cable modem on line</li> <li>• doing DCC</li> <li>• <b>show cable modem</b></li> </ul> <p>Workaround: There is no workaround.</p>
CSCsv94090	<p>Symptom: When using modem-method load balancing, the DOCSIS 3.0 modems are counted as single modem per downstream channel. This results in many DOCSIS 3.0 modems on 1 channel, which means DOCSIS 2.0 modems will get pushed off, leaving that channel only for bonded traffic (in the case that Dynamic Bandwidth Sharing is in use, with the SPA channel given 90% remaining ratio for both types of traffic i.e. best effort). If the D3.0 modem was counted as a single modem on the Bonded Group of channels (that is on 3 channels) then they would not influence the movement of D2.0 modems as the D3.0 modems would appear to be equally spread across the SPA channels.</p> <p>Conditions: D3.0 modem with load balancing enabled.</p> <p>Workaround: There is no workaround.</p>
CSCsv95506	<p>The following tracebacks are observed when cable modem comes online. The syslog messages did not indicate the trigger of tracebacks.</p> <pre> SLOT 7/0: Nov 17 19:29:15.257 CST: %ALIGN-3-TRACE: -Traceback= 6028F5AC 60520738 6028CA08 6028CCCC 6021D4B0 6021DE2C 6021E0B8 00000000 SLOT 7/0: Nov 17 19:29:15.257 CST: %ALIGN-3-TRACE: -Traceback= 6028F5C4 60520738 6028CA08 6028CCCC 6021D4B0 6021DE2C 6021E0B8 00000000 SLOT 7/0: Nov 17 19:29:15.257 CST: %ALIGN-3-TRACE: -Traceback= 6028F604 60520738 6028CA08 6028CCCC 6021D4B0 6021DE2C 6021E0B8 00000000 SLOT 7/0: Nov 17 19:29:15.257 CST: %ALIGN-3-TRACE: -Traceback= 6028F648 60520738 6028CA08 6028CCCC 6021D4B0 6021DE2C 6021E0B8 00000000 SLOT 7/0: Nov 17 19:29:15.257 CST: %ALIGN-3-TRACE: -Traceback= 6028F680 60520738 6028CA08 6028CCCC 6021D4B0 6021DE2C 6021E0B8 00000000 SLOT 7/0: Nov 17 19:29:15.257 CST: %ALIGN-3-TRACE: -Traceback= 6028F6B8 60520738 6028CA08 6028CCCC 6021D4B0 6021DE2C 6021E0B8 00000000 SLOT 7/0: Nov 17 19:29:15.257 CST: %ALIGN-3-TRACE: -Traceback= 60215538 6028F6F8 60520738 6028CA08 6028CCCC 6021D4B0 6021DE2C 6021E0B8 SLOT 7/0: Nov 17 19:29:15.257 CST: %ALIGN-3-TRACE: -Traceback= 60215558 6028F708 60520738 6028CA08 6028CCCC 6021D4B0 6021DE2C 6021E0B8                     </pre> <p>Condition: Tracebacks are observed when the REG_REQ_MP message is used to register a cable modem.</p> <p>Workaround: There is no workaround.</p>

**Table 28** *Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsv95785	<p>Symptom: The wideband interface command wrongly displays &lt;0-23&gt; range for ports and &lt;0-3&gt; range for subslot/bay.</p> <p>Conditions: This issue is observed in the routers running Cisco IOS 12.3(23)BC, 12.2(33)SCA, and 12.2(33)SCB.</p> <p>Workaround: There is no workaround.</p>
CSCsm27071	<p>Symptom: Memory leak occurs with certain socket applications.</p> <p>Condition: Occurs with the skinny socket server process after repeated rejected phone registrations.</p> <p>Workaround: There is no workaround.</p>
CSCsv24663	<p>Symptom: When cable metering is enabled, the following scheduler thrashing error message has been seen in PRE log related to all cable linecards:</p> <p>SLOT 5/0: Oct 14 23:31:32 EDT: %SCHED-3-THRASHING: Process thrashing on watched message event.</p> <p>-Process= "CMTS METERING Collection Process", ipl= 4, pid= 105</p> <p>-Traceback= 6013579C 60135880 60585190 60584C58 601134B4 60113498</p> <p>Conditions: Above problem has been observed only when 'cable metering' is configured on a Cisco uBR10012 router with PRE2.</p> <p>Workaround: There is no workaround.</p>

**Table 28 Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)**

DDTS ID Number	Description
CSCsu88884	<p>Symptom: All the upstreams in a slot show <i>Frequency not set</i>, as follows:</p> <pre>interface Cable&lt;#&gt; cable downstream frequency &lt;#&gt; no cable downstream rf-shutdown cable upstream 0 spectrum-group &lt;#&gt; no cable upstream 0 shutdown cable upstream 1 spectrum-group &lt;#&gt; no cable upstream 1 shutdown cable upstream 2 spectrum-group &lt;#&gt; no cable upstream 2 shutdown cable upstream 3 spectrum-group &lt;#&gt; no cable upstream 3 shutdown Cable&lt;#&gt; Downstream is up Frequency &lt;#&gt; MHz, Channel Width &lt;#&gt; MHz, &lt;#&gt;-QAM, Symbol Rate &lt;#&gt; Msp &lt;..&gt; Cable&lt;#&gt; Upstream 0 is down Frequency not set, Channel Width &lt;#&gt; MHz, &lt;#&gt;-QAM Symbol Rate &lt;#&gt; Msp This upstream is mapped to physical port &lt;#&gt; Spectrum Group &lt;#&gt; &lt;..&gt; Cable&lt;#&gt; Upstream 2 is down Frequency not set, Channel Width &lt;#&gt; MHz, &lt;#&gt;-QAM Symbol Rate &lt;#&gt; Msp This upstream is mapped to physical port &lt;#&gt; Spectrum Group &lt;#&gt; &lt;..&gt;</pre> <p>Condition: This occurs after the following OIR sequence:</p> <ol style="list-style-type: none"> <li>1. OIR compatibility configured for the slot</li> <li>2. Configuration saved</li> <li>3. Cable powered off</li> <li>4. MC5x20U card pulled out and MC5x20H card inserted</li> <li>5. Cable powered on</li> </ol> <p>Workaround: Reload the CMTS.</p>
CSCsu77329	<p>Symptom: Line cards crash after the line card switchover under specific conditions.</p> <p>Conditions: When the Subscriber Traffic Management (STM) enforce-rules are configured and then removed, the active line cards crash after a LC switchover.</p> <p>Workaround: Delete all modems being monitored by the deleted enforce-rule.</p>
CSCsv04901	<p>Symptom: When the Cisco MC520H line card is in normal operation condition, modems on one or a few upstreams get into a bad state, and all modems on the affected upstreams go offline, while other upstreams are still functioning.</p> <p>Condition: There is traffic on the upstreams. This affects only the MC520H line cards on all releases.</p> <p>Workaround: Run the <b>shut/no shut cable interface</b> command on the affected upstreams.</p>

**Table 28** *Resolved Caveats for Cisco IOS Release 12.3(23)BC6 (continued)*

DDTS ID Number	Description
CSCsu76930	<p>Symptom: When setting the Fragment-force 2000 the upstream performance drops to zero. There is no upstream thought-put.</p> <p>Conditions: Problem is found only on the Cisco MC5X20S line card running Cisco IOS 12.3(23)BC1.</p> <p>Workaround: Put Fragment-force to Frag-force 1987 for best performance.</p>
CSCsu95526	<p>Symptom: Cable modems go offline due to a very low SNR value when PRE-Equalization is enabled.</p> <p>Conditions: This issue is observed when the modulation profile IUC1 (request) burst size is 1 minislot.</p> <p>Workaround: Calculate the request (IUC1) burst size based on the modulation profile, symbol rate, and minislot size configuration. Make sure that request burst profile is at 2 minislot in duration.</p>
CSCsr74034	<p>Symptom: Ironbus restarts have been observed on the Cisco uBR10012 router due to ironbus link status 0x1180 errors. You observe the following messages in the PRE log:</p> <pre data-bbox="613 898 1503 1115"> ----- 811468: Jun 17 03:10:17.233 UTC: slotindex is 8. 811469: Jun 17 03:10:17.233 UTC: IB Link status: 00001180 811470: Jun 17 03:10:17.233 UTC: %C10KEVENTMGR-1-IRONBUS_FAULT: Ironbus Event 5/0, Restarting Ironbus 811471: Jun 17 03:10:17.645 UTC:%C10KEVENTMGR-1-IRONBUS_SUCCESS: Ironbus Event 5/0, Restart Successful ----- </pre> <p>The ironbus link status 0x1180 error will trigger an line card switchover on uBR10012s configured with N 1 redundancy. The ironbus restart is fast enough to keep modems online and has negligible affect to customers on uBR10012s without N+1 redundancy.</p> <p>Conditions: This ironbus link status 0x1180 error has only been observed on slot 5/0 with the following hardware configuration. - Working Cisco uBR10-MC520H line card in slot 5/0 (the problem has not been reported on the Cisco uBR10-MC520U/S cards) - Active PRE2 in slot A (the problem has not been reported on a PRE1) Cisco Systems is still investigating the root cause of the ironbus link status 0x1180 error.</p> <p>Workaround: There are two workarounds for ironbus link status 0x1180 error 1. Use Active PRE2 in slot B 2. Do not use a Cisco uBR10-MC520H in slot 5/0 Customers should not RMA any equipment due to the ironbus link status 0x1180 error. Cisco Systems has not confirmed that this is a hardware issues and would need to identify the faulty hardware (e.g., PRE2, Cisco uBR10-MC520H, chassis) if it is a hardware issue.</p>

## Open Caveats for Release 12.3(23)BC5

Table 29 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(23)BC5.

**Table 29** Open Caveats for Cisco IOS Release 12.3(23)BC5

DDTS ID Number	Description
CSCso16183	<p>Symptom: SNMP may report different speeds and modulation types for upstream channels configured for the same type of modulation. The ifSpeed variable reported in SNMP conforms to 16QAM at 10.24Mbps on some interfaces but shows as QPSK at 5.12Mbps on others.</p> <p>Changing the load balance groups still results in the same issue.</p> <p>Condition: This issue is observed on a Cisco uBR10012 router with cable linecard interfaces configured for 16QAM (modulation profile 24) with the following configuration:</p> <ul style="list-style-type: none"> <li>• Spectrum-groups and upstream load balancing configured</li> <li>• Two upstream channels in the same US load balance group, and</li> <li>• Two upstreams in the same spectrum group.</li> </ul> <p>Although the <b>show controller</b> command reports 16QAM for all upstream channels, SNMP reports QPSK for some and 16QAM for others.</p> <p>Workaround: There is no workaround.</p>
CSCsu44606	<p>Symptom: Duplicate traps are generated when configuring SNMP traps for cable billing operations.</p> <p>Workaround: There is no workaround.</p>
CSCsr54283	<p>Symptom: When the active DTI is reset, SNMP traps are not generated.</p> <p>Workaround: Enable the following commands so that Syslog forwards the traps to SNMP:</p> <pre>snmp-server enable traps syslog snmp-server enable traps fru-ctrl</pre> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="text-align: center; margin-right: 10px;">   <b>Caution</b> </div> <div> <p>Enabling the above commands may overload the Network Management System (NMS) in the network.</p> </div> </div>
CSCso87178	<p>Symptom: Modems in random upstream (US) ports go offline and return to online status in a few minutes. This is recorded and displayed as output of the <b>show cable flap-list</b> command.</p> <p>Condition: This has been reported from newly installed Cisco uBR10012 Routers having Cisco uBR10-MC5X20H linecard.</p> <p>Workaround: Wait for a few minutes for automatic correction.</p>
CSCso59575	<p>Symptom: CMTS truncates rfs witch name, when the name is more than 30 characters.</p> <p>Workaround: There is no workaround.</p>

**Table 29** *Open Caveats for Cisco IOS Release 12.3(23)BC5 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsr78306	<p>Symptom: Customer premises equipment (CPE) traffic sent to the wrong cable modem.</p> <p>Conditions: This occurs when:</p> <ul style="list-style-type: none"> <li>• There is spoofing of the CPE address</li> <li>• ARP packets are sent from the CPE</li> </ul> <p>Workaround: Delete the modem from the database.</p>
CSCs150048	<p>Symptom: Modems without minimum and maximum DS rate configured fail to register on modular-cable downstreams even when they use config files that have downstream llq (max downstream latency) set.</p> <p>Condition: These modems are stuck in reject(c) state.</p> <p>Workaround: Configure minimum and maximum DS rate in the downstream service flow encoding in the config file.</p>
CSCsq64227	<p>Symptom: The number of downstream PHS rules for a cable MAC domain stays the same even though more downstreams are added to the MAC domain (via modular downstreams).</p> <p>Workaround: There is no workaround.</p>
CSCsu53992	<p>Symptom: Following message is seen in the output of <b>show cable modem</b> command:</p> <pre>Warning: Zero Blaze index for SFID 173</pre> <p>Workaround: There is no workaround. However, this is a cosmetic issue and does not affect the data flow.</p>
CSCsl35163	<p>Symptom: The range-backoff configuration value changes from "range-backoff 3 6" to "range-backoff automatic" for upstream in a frequency stacking scenario.</p> <p>This change is noticed after the following commands are executed to un-configure and re-configure the cable interface.</p> <ol style="list-style-type: none"> <li><b>1. cable upstream max-ports 6</b></li> <li><b>2. no cable upstream max-ports</b></li> <li><b>3. cable upstream max-ports 6</b></li> </ol> <p>Workaround: There is no workaround.</p>
CSCsl49206	<p>Symptom: If the associated HA <b>ip host</b> commands are removed followed by PRE switchovers from PREA to PREB and then from PREB to PRE, after re-configuring the Global HA commands, all modems disappear, re-range and then come back online.</p> <p>Workaround: There is no workaround.</p>
CSCsm00986	<p>Symptom: Traceback occurs when the HCCP (Hot Standby Connection-to-Connection Protocol) member is removed through the console and when the <b>sh hccp channel-switch</b> command is run from the VTY session almost simultaneously.</p> <p>Workaround: There is no workaround.</p>

Table 29 Open Caveats for Cisco IOS Release 12.3(23)BC5 (continued)

DDTS ID Number	Description
CSCso21260	<p>Symptom: When configuring certain rfs witch snmp-community string as a redundancy sub-option, the CMTS does not automatically create the corresponding <b>snmp-server community &lt;password&gt; view hccp_chansw_snmp_view RW</b> entry resulting in the line card switchover failure.</p> <p>Workaround: There is no workaround.</p>
CSCso34318	<p>Symptom: The Cisco uBR10012 router allows the entry of 128 characters for SNMP community string, whereas the internal SNMP agent truncates this to 64 characters.</p> <p>Workaround: Use only 64 characters or less for SNMP community strings in the CMTS.</p>
CSCsr40228	<p>Symptom: CST-WBHA-BC2 modems go offline after multiple linecard and PRE switchovers.</p> <p>Condition: This issue is observed when the following steps are performed:</p> <ol style="list-style-type: none"> <li>1. Switchover from 7/1 to 5/1</li> <li>2. Switchover from PRE-A to PRE-B</li> <li>3. Revertback linecard from 5/1 to 7/1</li> <li>4. Switchover from 5/0 to 5/1</li> <li>5. Switchover from PRE-B to PRE-A</li> </ol> <p>The modems go offline at this stage.</p> <p>Workaround: There is no workaround.</p>
CSCsr45093	<p>Symptom: Protect interfaces are protecting two different working cards at the same time.</p> <p>Conditions: This issue occurs when some standby interfaces are shut down and some cards are out of service (crash, power off, etc).</p> <p>Workaround: Use <b>no shutdown</b> command at the working interface and revert from protect card to working card.</p>

**Table 29** *Open Caveats for Cisco IOS Release 12.3(23)BC5 (continued)*

DDTS ID Number	Description
CSCsj97292	<p>Symptom: Under rare conditions, a Hot Standby Connection-to-Connection Protocol (HCCP) switchover and revertback can cause all JIBs to shut down, the UP convertor to be disabled, and all modems to drop. This issue is not necessarily a cable modem termination system (CMTS) problem; sometimes it can be triggered by HCCP issues as well.</p> <p>To diagnose this problem:</p> <ol style="list-style-type: none"> <li>1. Enter the <b>show controller</b> <i>x/y/z</i> command. Note that the output will display: “i Disable”.</li> <li>2. Enter the <b>show hccp detail</b> command. Note that the Member Loading output count is not 0.</li> </ol> <p>Workaround: Recover the modems from offline status by performing the following steps:</p> <ol style="list-style-type: none"> <li>1. Remove the protect member.</li> <li>2. Remove the problematic working member.</li> <li>3. Normalize the new standalone card and get the modems back online. (Note that after the modems are back online, the hccp count value will still be greater than 0 5.)</li> <li>4. Decide whether you want to add the working and protect members back.</li> <li>5. Schedule a maintenance window to recover the hccp Member Loading non 0 count 1.</li> </ol> <p>Recover the hccp Member Loading non 0 count 1 by performing the following steps:</p> <ol style="list-style-type: none"> <li>1. Reset the secondary PRE to re-synchronize the database.</li> <li>2. Check that the secondary PRE is working.</li> <li>3. Perform a switchover to the PRE.</li> <li>4. Enter the <b>show hccp detail</b> command. The Member Loading output count should be 0 5.</li> <li>5. Perform the CLC switchover now to make sure HCCP works as designed. (This step assumes that you have the line card already put back into the global HCCP configuration.)</li> </ol>
CSCsr59753	<p>Symptom: In certain Cisco IOS releases, mixed docsis mode (atdma-tdma) can only achieve 40 UGS for an upstream.</p> <p>Condition: This may be the result of mixed mode and modems.</p> <p>Workaround: There is no workaround.</p>
CSCsu36225	<p>Symptom: Two upstream ports on the same PHY receiver of a Cisco uBR10-MC5X20H linecard show signal-to-noise ratio (SNR) degradation of about 10 dB.</p> <p>Condition: This occurs due to ingress-noise cancellation.</p> <p>Workaround: There is no workaround.</p>

**Table 29 Open Caveats for Cisco IOS Release 12.3(23)BC5 (continued)**

DDTS ID Number	Description
CSCsu12182	<p>Symptom: <b>show controllers</b> command does not display the Downstream RF power output or the Downstream Frequency, for the Downstreams that are associated by the same JIB (chipset), as given below:</p> <pre>Cable6/1/2 Upconverter is Enabled Output is Enabled Model: Serial Number: HW Rev: SW Rev: 204, NVRAM Rev: 021 ECI number FFFFFFFF Downstream Frequency 0.0000 MHz RF Power 0.0 dBmV</pre> <p>Condition: This occurs in a Cisco uBR10012 router with Cisco uBR10-MC5X20U card.</p> <p>Workaround: Use the cable power command to power off and on the slot location where the line card is installed.</p>
CSCso96838	<p>Symptom: Secondary PRE2 crashes.</p> <p>Condition: This issue is observed when the following exceptions are run:</p> <ul style="list-style-type: none"> <li>• no exception-slave core-file ubr3</li> <li>• no exception-slave dump 172.18.98.28</li> <li>• no exception core-file ubr3, and</li> <li>• no exception dump 172.18.98.28.</li> </ul> <p>Workaround: Do not remove the exception.</p>
CSCso60646	<p>Symptom: When the last rf-channel is removed from a wideband-cable interface, the interface's bandwidth is not reset to zero as per the <b>show interface wideband-cable x/y/z:w downstream</b> command. This is a cosmetic issue</p> <p>Workaround: There is no workaround.</p>
CSCsu74681	<p>Symptom: The <b>show cable load-balance</b> command displays details of the wideband cable interfaces (upstream and downstream) twice in the command output.</p> <p>Condition: This issue is observed in a wideband cable setup with 3.0 DOCSIS cable modems and non-DOCSIS 3.0 cable modems.</p> <p>Workaround: You can keep track of the aggregate statistics for the interface manually.</p>
CSCso63567	<p>Symptom: When a cable modem is locked with primary channel from SPA, voice call tone dropout of 4500~5000ms was observed during bulk calls.</p> <p>Condition: Difficult to be recreated.</p> <p>Workaround: There is no workaround.</p>

**Table 29**      **Open Caveats for Cisco IOS Release 12.3(23)BC5 (continued)**

DDTS ID Number	Description
CSCsr75525	<p>Symptom: Incorrect power values for Power Entry Modules (PEM) displayed by the <b>show controllers clock-reference</b> command.</p> <p>While PEM0 + PEM1 should not be higher than 2400, a single PEM's power exceeds that value.</p> <p>Condition: Cisco uBR10012 TCC card is used. Re-seating the card does not solve the problem.</p> <p>Workaround: There is no workaround.</p>
CSCsr43079	<p>Symptom: When standby PRE is reloaded, the current STM monitoring details are not displayed correctly in the output of the <b>show cable qos enforce-rule verbose</b> command.</p> <p>Condition: This occurs if standby PRE is reloaded when active PRE is up. This does not occur if the standby PRE is not reloaded. This issue does not affect STM functionality. The Standby PRE will get the correct monitoring details in the next monitoring period.</p> <p>Workaround: There is no workaround.</p>
CSCsu65409	<p>Symptom: Cable Modems are penalized at random for a few seconds into the maintenance window, even before they exceed the limits.</p> <p>Condition: This occurs in CMTS environments using Subscriber Traffic Management (STM).</p> <p>Workaround: There is no workaround.</p>
CSCsq01701	<p>Symptom: Resetting the wideband cable modems make them come w-online and the upstream STM enforce- rule configuration does not shape their traffic as expected.</p> <p>Condition: This issue can be seen if modems are in penalty state and for some reason get reset at that time. Normally modems in penalty state do not get reset. If they get reset, they will come online and not shape the traffic only for that penalty.</p> <p>Workaround: There is no workaround.</p>

**Table 29** Open Caveats for Cisco IOS Release 12.3(23)BC5 (continued)

DDTS ID Number	Description
CSCso57024	<p>Symptom: The Cisco vendor-specific "Wideband Channel ID" option (vendor-specific option 14) does not work.</p> <p>Condition: This issue is observed when using a recent version of Scientific Atlanta wideband DPC2505 modem with the Cisco uBR10012 router.</p> <p>Workaround: There is no workaround.</p>
CSCsu88884	<p>Symptom: All the upstreams in a slot show <i>Frequency not set</i>, as follows:</p> <pre>interface Cable&lt;#&gt; cable downstream frequency &lt;#&gt; no cable downstream rf-shutdown cable upstream 0 spectrum-group &lt;#&gt; no cable upstream 0 shutdown cable upstream 1 spectrum-group &lt;#&gt; no cable upstream 1 shutdown cable upstream 2 spectrum-group &lt;#&gt; no cable upstream 2 shutdown cable upstream 3 spectrum-group &lt;#&gt; no cable upstream 3 shutdown</pre> <p>Cable&lt;#&gt; Downstream is up Frequency &lt;#&gt; MHz, Channel Width &lt;#&gt; MHz, &lt;#&gt;-QAM, Symbol Rate &lt;#&gt; Msp Mps &lt;..&gt;</p> <p>Cable&lt;#&gt; Upstream 0 is down Frequency not set, Channel Width &lt;#&gt; MHz, &lt;#&gt;-QAM Symbol Rate &lt;#&gt; Msp This upstream is mapped to physical port &lt;#&gt; Spectrum Group &lt;#&gt; &lt;..&gt;</p> <p>Cable&lt;#&gt; Upstream 2 is down Frequency not set, Channel Width &lt;#&gt; MHz, &lt;#&gt;-QAM Symbol Rate &lt;#&gt; Msp This upstream is mapped to physical port &lt;#&gt; Spectrum Group &lt;#&gt; &lt;..&gt;</p> <p>Condition: This occurs after the following OIR sequence:</p> <ol style="list-style-type: none"> <li>1. OIR compatibility configured for the slot</li> <li>2. Configuration saved</li> <li>3. Cable powered off</li> <li>4. MC5x20U card pulled out and MC5x20H card inserted</li> <li>5. Cable powered on</li> </ol> <p>Workaround: Reload the CMTS.</p>

## Resolved Caveats for Release 12.3(23)BC5

Table 30 lists only severity 1 and 2 caveats and select severity 3 resolved caveats for Cisco IOS Release 12.3(23)BC5.

**Table 30 Resolved Caveats for Cisco IOS Release 12.3(23)BC5**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsu30702	Symptom: SNMP Polling does not respond to requests. Workaround: Use CLI command to clear ARP table. Do not use the MIB object <b>sysClearARP</b> to clear the ARP table.
CSCsu81980	Symptom: When a Cisco uBR10012 router running Cisco IOS release 12.3 boots up, some IPC connections between Cisco uBR10-MC5X20 cards do not come up. Condition: This occurs when the system is fully loaded, and the CPU usage is high or the Backplane Ethernet (BPE) usage is high. Workaround: Reload the affected Cisco uBR10-MC5X20 card, or do a PRE switchover.
CSCsr47518	Symptom: The Cisco uBR10012 router reloads due to bus error. Workaround: There is no workaround.
CSCsu62059	Symptom: During error conditions, output of the <b>show diagnostic status</b> command shows incorrect subslot status. Condition: This occurs when a line card is loaded with an invalid field diagnostic image. Workaround: Load the line card with the correct field diagnostic image.
CSCsr50501	Symptom: Spurious memory traceback observed inubr10k CMTS while testing Field Diagnostics. Condition: After loading the field diagnostic image to the line card, starting and stopping the Online Offline Diagnostics (OOD) tests sometimes cause the PRE to fail. Workaround: There is no workaround.
CSCsr45883	Symptom: A linecard reset occurs if the card is loaded with an invalid URL for the field diagnostic image. Condition: This occurs when the URL/disk (field diagnostic image location) is incorrect in the following command: <b>diagnostic load subslot &lt;no&gt; &lt;url&gt;</b> Workaround: Make sure that the correct URL/disk is specified while loading the field diagnostic image to the linecard.
CSCsu85219	Symptom: The indexes maintained for the 24 RF-channel SPA are not cleared, after the modems using SPA downstream are reset or deleted by the command: <b>clear cable modem cx/y/z all reset/delete</b> Condition: This occurs when the Cisco uBR10-MC5X20S/U/H host of the modular cable interface is using a non-default downstream channel ID. Workaround: Use the following command: <b>clear cable modem all reset</b>

Table 30 Resolved Caveats for Cisco IOS Release 12.3(23)BC5 (continued)

DDTS ID Number	Description
CSCsr12024	<p>Symptom: With the wideband multicast BPI and wideband host HA configuration, the linecard crashes while syncing BPI data.</p> <p>Condition: This occurs when there are a large number of BPI multicast keys in wideband host data. It causes linecard memory corruption and eventually crashes the line card.</p> <p>Workaround:</p> <ul style="list-style-type: none"> <li>• Disable wideband multicast BPI configuration</li> </ul> <p style="text-align: center;">OR</p> <ul style="list-style-type: none"> <li>• Disable wideband host HA configuration.</li> </ul>
CSCsr30738	<p>Symptom: SLOWRPC error message is generated in IPC code while booting the Cisco uBR10012 router.</p> <p>Workaround: There is no workaround.</p>
CSCsr52709	<p>Symptom: Service flow counts are not updated for downstream service flows handled by the 24 rfchannel SPA. As a result dynamic service flows for voice may be torn down when the T8 (inactivity) timer expires.</p> <p>Condition: This issue is observed when SPA in bay 0 is inserted but the Gigabit Ethernet link is disconnected or offline.</p> <p>Workaround: Ensure that the SPA0 Gigabit Ethernet link is up whenever SPA 0 exists.</p>
CSCsr69249	<p>Symptom: Cable modems drop offline or lose PacketCable Multimedia (PCMM) call, after a linecard switch over or a revert back.</p> <p>Condition: Channel Grouping Domain (CGD) is configured on CMTS.</p> <p>Workaround: There is no workaround</p>
CSCsu08086	<p>Symptom: All modems go offline on the protect port after a linecard switchover.</p> <p>Condition: <b>cable default-phy-burst</b> is configured with a value other than the default (2000).</p> <p>Workaround:</p> <ul style="list-style-type: none"> <li>• Issue <b>shut/no shut</b> commands to the upstream port.</li> <li>• Configure <b>cable default-phy-burst</b> with the default value.</li> </ul>
CSCsr48745	<p>Symptom: Some modems go offline, after the linecard switchover or revertback, and upstream phy register shows late map issue.</p> <p>Condition: This occurs when the dynamic map-advance safety is configured with a small value.</p> <p>Workaround: Increase the value of dynamic map-advance safety or use static map-advance.</p>

**Table 30** *Resolved Caveats for Cisco IOS Release 12.3(23)BC5 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsr27586	<p>Symptom: Traceback is seen when VRF configuration is removed.</p> <p>Condition: This occurs when:</p> <ul style="list-style-type: none"> <li>• Cable modem is w-online on the modular interface</li> <li>• Switch over from PRE-A to PRE-B</li> <li>• Issue the command: <b>clear cable modem all del</b></li> </ul> <p>Workaround: There is no workaround.</p>
CSCsr54991	<p>Symptom: When SX SFP is used, input drop and ignore counters for Half Height Gigabit Ethernet (HHGE) linecard keep incrementing. This happens even if there is no traffic.</p> <p>Workaround: If possible use Copper SFP instead of SX SFP.</p> <p>OR:</p> <ol style="list-style-type: none"> <li>1. Disconnect or remove the SFP from the HHGE</li> <li>2. Issue the command <b>hw sub reset</b></li> <li>3. Wait for the HHGE to come up (it takes one minute).</li> <li>4. Plug in the SFP.</li> </ol> <p> <b>Note</b> The above workaround disrupts the user traffic.</p>
CSCsr70184	<p>Symptom: Access to a gate is refused due to exceeded activity-count even when the subscriber has no gate assigned.</p> <p>Condition: Packetcable was running.</p> <p>Workaround: Increase the value of the maximum calls allowed for a user in the BTS server. This will permit calls to be accepted again. However, a reload is necessary to reset the counter.</p>
CSCsr07340	<p>Symptom: Backup TCC card may experience a reload (IPCOIR-3-TIMEOUT on TCC card).</p> <p>Workaround: There is no workaround.</p>

**Table 30 Resolved Caveats for Cisco IOS Release 12.3(23)BC5 (continued)**

DDTS ID Number	Description
CSCsr56659	<p>Symptom: Secondary PRE2 crashes with the following messages in the log related to multiple cable modem mac-addresses:</p> <pre data-bbox="573 394 1479 520">%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow, cr10k_rp_ha_parse_ds_srv_flow: DSA sfid 14412 failed to create new sfid</pre> <p>Workaround:</p> <p>The reset of a cable linecard will result in the service flow state database being left in an inconsistent state on the secondary PRE. Reload the Secondary PRE after the linecard reset.</p> <p>If the secondary PRE were to become the Primary PRE when a linecard reset occurred, the service flow state database on the newly active Primary PRE will be in an inconsistent state. This can be set right by performing a failover of the PRE.</p>
CSCsr21171	<p>Symptom: While running the <b>show cable modem</b> or related commands the following warning is displayed:</p> <pre data-bbox="573 909 1008 930">Warning: Zero Blaze index for SFID</pre> <p>When the cable modem/subinterface is in this state, the stats counters for the subinterface report invalid numbers. However, the traffic to the cable modem is not impacted.</p> <p>Workaround: Reset the cable modem during maintenance windows.</p>
CSCsg81770	<p>Symptom:</p> <p>A subinterface with ifIndex=62 does not show up in the ifMIB output.</p> <p>Condition:</p> <p>When the router is configured such that the ifIndex value of 62 gets assigned to a subinterface (non-HWIDB), the interface may not show up in the ifMIB output.</p> <p>Workaround:</p> <p>Enable ifIndex persistence using the <b>snmp ifindex persist</b> command, when ifIndex 62 is given to a HWIDB. You can also configure the router's interfaces in such a way that ifIndex 62 is given to a HWIDB.</p> <div data-bbox="573 1482 621 1518" style="text-align: left;">  </div> <p><b>Note</b> You will need to reload the Cisco uBR10012 router if this condition is encountered.</p>
CSCso39755	<p>Symptom: Some voice call downstream service flow counters increase drastically after a linecard switchover. It automatically drops to normal values but shoots up again, if the time between the consecutive execution of <b>show interface Cx/y/z service-flow xxx counters/qos</b> command is long enough.</p> <p>Condition: This occurs during race conditions.</p> <p>Workaround: There is no workaround.</p>

**Table 30** *Resolved Caveats for Cisco IOS Release 12.3(23)BC5 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsr88833	<p>Symptom: DOCSIS 3.0 modems are currently counted in the load balancing algorithm, but do not support Dynamic Channel Change (DCC). This implies that across 4 channels (primary and bonded sharing DOCSIS 3.0 and DOCSIS 2.0), you will end up with a high modem count on one channel, with little or no DOCSIS 2.0 modems on it. If this channel is on a linecard, it will not carry bonded traffic, therefore resulting in an under utilized downstream channel.</p> <p>Condition: This occurs while load balancing by modem-count method. Utilization based load balancing is preferable, but does not work in conjunction with Dynamic Bandwidth Selection (DBS).</p> <p>Workaround: Place the primary channel for DOCSIS 3.0 modems on an SPA channel, so that it carries only bonded traffic. The other channels now carry DOCSIS 2.0 traffic.</p>
CSCsr92986	<p>Symptom: Cisco Network Registrar (CNR) is not shown for frequency stacked upstreams. For example, if the following configuration is used on a 1x4 MAC domain:</p> <pre data-bbox="613 846 1060 894">cable upstream 0 connector 0 shared cable upstream 1 connector 0 shared</pre> <p>Only upstream 0 will show a CNR value in the output of the <b>show controller cx/y/z upstream</b> command. Upstream 1 will show only a MER value. This can break CNR based frequency hopping, as the output of the <b>show cable hop thresholds</b> command does not display a CNR for the affected upstream.</p> <p>Workaround: The only known workaround is to avoid frequency stacking.</p>

**Table 30 Resolved Caveats for Cisco IOS Release 12.3(23)BC5 (continued)**

DDTS ID Number	Description
CSCsu77729	<p>Add Error Packet Capture Debug functionality for 24 RF channel SPA. This helps in getting packets log from SPA, in case of SPA downstream issues.</p> <p>Sample output of <b>show controllers modular-cable x/0/y</b>, with NO error packets captured:</p> <pre>Router#show controllers modular-Cable 1/0/1   b reading WBCMTS DOCSIS SPA temperature sensor 0, reading: 25C/77F WBCMTS DOCSIS SPA temperature sensor 1, reading: 25C/77F</pre> <p><b>Error Packets Captured on Blaze SPI Interface:</b></p> <pre>Timestamp IntStat Len BlazeHeader Detail Packet Content: (first 80 bytes, hex format) ----- Start of SPA1 Black Box -----</pre> <p>Sample output of <b>show controllers modular-cable x/0/y</b> command, with error packets already been captured:</p> <pre>Router#show controllers modular-Cable 1/0/0 SPA 0 is present status LED: [green] Host 12V is enabled and is okay. Power has been enabled to the SPA. SPA reports power enabled and okay. SPA reports it is okay and is NOT held in reset. ..... &lt;&lt;&lt; text omitted&gt;&gt;&gt;</pre> <pre>WBCMTS DOCSIS SPA temperature sensor 0, reading: 26C/78F WBCMTS DOCSIS SPA temperature sensor 1, reading: 25C/77F</pre> <p><b>Error Packets Captured on Blaze SPI Interface:</b></p> <pre>Timestamp IntStat Len BlazeHeader 000:00:12:49.190 C0000808 1510 00 00 00 00 01 00 00 00 00 00 00 00 00 0F C2 00 000:00:13:04.948 C0000808 796 00 00 00 00 01 00 00 00 00 00 00 00 00 0F C2 00 000:00:13:09.468 C0000808 60 00 00 00 00 01 00 00 00 00 00 00 00 00 0F C2 00 000:00:13:14.320 C0000808 26 00 00 00 00 01 00 00 00 00 00 00 00 00 0F C2 00 000:00:13:18.088 C0000808 496 00 00 00 00 01 00 00 00 00 00 00 00 00 0F C2 00</pre>

**Table 30** Resolved Caveats for Cisco IOS Release 12.3(23)BC5 (continued)

DDTS ID Number	Description
CSCsu77729 (Continued)	<p>Detail Packet Content: (first 80 bytes, hex format)</p> <pre>[Entry 00] 0x00: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 0F C2 00 0x10: 00 1C 9C 24 01 E0 2F 00 00 01 00 00 00 00 00 00 0x20: 00 0A 00 00 03 04 FD 00 00 48 03 FC 00 00 00 00 0x30: 00 00 00 00 00 00 00 05 00 00 00 00 80 06 12 78 0x40: 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 00  [Entry 01] 0x00: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 0F C2 00 0x10: 00 1C 9C 24 01 E0 2F 00 00 01 00 00 00 00 00 00 0x20: 00 0A 00 00 03 04 FD 00 00 48 03 FC 00 00 00 00 0x30: 00 00 00 00 00 00 00 05 00 00 00 00 80 06 12 78 0x40: 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 00  [Entry 02] 0x00: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 0F C2 00 0x10: 00 1C 9C 24 01 E0 2F 00 00 01 00 00 00 00 00 00 0x20: 00 0A 00 00 03 04 FD 00 00 48 03 FC 00 00 00 00 0x30: 00 00 00 00 00 00 00 05 00 00 00 00  [Entry 03] 0x00: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 0F C2 00 0x10: 00 1C 9C 24 01 E0 2F 00 00 01  [Entry 04] 0x00: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 0F C2 00 0x10: 00 1C 9C 24 01 E0 2F 00 00 01 00 00 00 00 00 00 0x20: 00 0A 00 00 03 04 FD 00 00 48 03 FC 00 00 00 00 0x30: 00 00 00 00 00 00 00 05 00 00 00 00 80 06 12 78 0x40: 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 00</pre> <p>----- Start of SPA0 Black Box -----</p> <p>Description of the output:</p> <p>There are two parts of the output addition: SPA temperature readings and error packets capture information, added near the end of the command output, before the Black Box console log part.</p> <ol style="list-style-type: none"> <li>1. First two lines are the current temperature readings of the two sensors on SPA.</li> <li>2. Next is the error packets capture information</li> </ol> <p>A brief description of maximum 16 captured error packets is displayed, including:</p> <ul style="list-style-type: none"> <li>- Timestamp of the capturing.</li> <li>- Interrupt state when packet is captured, which indicates the error type.</li> <li>- Packet length.</li> <li>- Blaze header part of the packet.</li> </ul> <p>This is followed by the details of the first 80 bytes of content of each error packet.</p>
CSCsu77134	<p>Symptom: Service class name field is empty in SAMIS records for deleted PCMM flow. SNMP MIB <b>docsQosServiceFlowLogServiceClassName</b> is also empty for these flows.</p> <p>Workaround: There is no workaround.</p>

**Table 30** *Resolved Caveats for Cisco IOS Release 12.3(23)BC5 (continued)*

DDTS ID Number	Description
CSCso81928	Symptom: Modems in penalty state due to STM configuration are not accessible after linecard switchover. Condition: This issue is seen in both legacy and wideband cable modems. Workaround: Reset the modem.
CSCso63716	Symptom: Output of the <b>show cable qos enforce-rule verbose</b> command does not display accurate details in some conditions. The problem is cleared after the first sample time. Condition: This occurs when there are multiple Cisco uBR10-MC5X20S/U/H cable linecards, having modems monitored with the same enforce rule. Workaround: There is no known workaround.

## Open Caveats for Release 12.3(23)BC4

[Table 31](#) lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(23)BC4.

**Table 31** *Open Caveats for Cisco IOS Release 12.3(23)BC4*

DDTS ID Number	Description
CSCso63105	Symptom: STM rate-limited traffic may exceed the limit. Condition: This issue is observed when rate-adapt is configured and flow is rate-adapt enabled. Workaround: Disable rate-adapt or change rate-adapt configuration so that flows that are eligible for STM are not eligible for rate-adapt.
CSCsr52709	Symptom: Service flow counts are not updated for downstream service flows handled by the 24 RF channel SPA. As a result dynamic service flows for voice may be torn down when the T8 (inactivity) timer expires. Condition: This issue is observed when SPA in Bay 0 is inserted but the GigE link is disconnected or offline. Workaround: Ensure that the SPA0 GigE link is up whenever SPA 0 exists.
CSCs180817	Symptom: The packets per second (pps) rate for a voice call is always less than 49 pps. Condition: Due to data traffic saturation in both upstream and downstream directions, the voice call pps is reduced to less than 49 pps. Workaround: There is no workaround.
CSCsq89541	Symptom: The Cisco uBR10012 router with PRE2 may cause on-net and off-net call rejection by CMTS due to GATE SET ERR and PKTCBL ERROR. Condition: This issue is observed when PRE2 is running on Cisco IOS 12.3(23)BC1 and later Cisco IOS releases in PacketCable environment. Workaround: There is no workaround.

**Table 31** *Open Caveats for Cisco IOS Release 12.3(23)BC4 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCs172140	<p>Symptom: Cable modems get stuck in init (io) because they cannot receive DHCP Offer and cannot proceed further.</p> <p>Conditions: This occurs occasionally on some modems.</p> <p>Workaround: Change the MAC address of the PC and get a new IP address using the <b>clear cable modem [mac-address] delete</b> command.</p>
CSCso81928	<p>Symptom: Modems in penalty state due to STM configuration are not accessible after linecard switchover.</p> <p>Condition: This issue is observed in both the legacy and wideband cable modems.</p> <p>Workaround: Reset the modem.</p>
CSCsq01701	<p>Symptom: Resetting the wideband cable modems make them come w-online and the upstream STM enforce- rule configuration does not shape their traffic as expected.</p> <p>Condition: This issue can be seen if modems are in penalty state and for some reason get reset at that time.</p> <p>Workaround: Normally modems in penalty state do not get reset. If they get reset, they will come online and not shape the traffic only for that penalty.</p>
CSCso82923	<p>Symptom: The cable interface configuration <b>cable dci-upstream-disable &lt;mac-address&gt; [enable disable]</b> appears to have no affect on the configuration.</p> <p>Condition: The MAC message is optional for modems and many modems ignore the MAC message.</p> <p>Workaround: Provision the cable modem with:</p> <ul style="list-style-type: none"> <li>• A DOCSIS 1.1 QOS profile of 10 Kbps upstream + 10kbps downstream</li> <li>• BPI + enabled, and</li> <li>• PC access denied.</li> </ul> <p>Do not use a max-cpe of 0 (unlimited CPE), use a max-cpe of 1.</p>
CSCso56190	<p>Symptom: The <b>show cable fiber-node</b> command does not display the description line entered under the fiber node in the running configuration mode.</p> <p>Condition: This issue is observed with following configuration:</p> <pre>R7508-uBR10K#sh cable fiber Fiber-Node 1   Local Primary Channels:   Remote RF Channels:     SPA 1/0/0: 0-3   FN Config Status: Configured (status flags = 0x1)   MDD Status: Valid  R7508-uBR10K#sh run   beg fiber-node cable fiber-node 1   description ALL DS on EQAM   downstream Modular-Cable 1/0/0 rf-channel 0-3   upstream Cable 5/0 connector 0</pre> <p>Workaround: Run the <b>show run   beg fiber-node</b> command.</p>

**Table 31**      **Open Caveats for Cisco IOS Release 12.3(23)BC4 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsk50223	<p>Symptom: The downstream modems failed to sync with the CMTS.</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running Cisco IOS 12.3(13a)BC6 or Cisco IOS 12.3(23)BC3 and later IOS releases with Cisco uBR10-MC5X20U-D linecard.</p> <p>Workaround: Power off/on the Cisco uBR10-MC5X20U-D linecard.</p>
CSCsr09380	<p>Symptom: Some modems fail to reach online(pt) state after a CMTS power cycle.</p> <p>Condition: If the hardware clock of the CMTS is set incorrectly, which may be outside the valid dates for the DOCSIS root certificate or EuroDOCSIS root certificate, the required / expected behavior is to reject all modems.</p> <p>Workaround: Correct the hardware clock on the processor card using the following commands:</p> <ul style="list-style-type: none"> <li>• <b>show clock</b></li> <li>• <b>set clock</b></li> <li>• <b>clock update-calendar</b></li> </ul> <p>Verify that the clock is properly set on the secondary PRE via the secondary PRE console.</p>
CSCso87178	<p>Symptom: Modems in random upstream(US) ports go offline and return to online status in a few minutes. This is recorded and displayed as output of the <b>show cable flap-list</b> command.</p> <p>Conditions: This has been reported from newly installed Cisco uBR10012 Routers having Cisco MC520H linecard.</p> <p>Workaround: Wait for a few minutes for automatic correction.</p>
CSCsm47906	<p>Symptom: Modems go offline after a severe noise in the Hybrid Fiber-Coaxial (HFC) end.</p> <p>Conditions: Severe noise on the HFC with pre-equalization enabled.</p> <p>Workaround: Disable pre-equalization using the <b>no cable upstream 0 equalization-coefficient</b> command.</p>

**Table 31** *Open Caveats for Cisco IOS Release 12.3(23)BC4 (continued)*

DDTS ID Number	Description
CSCsm12010	<p>Symptoms: With about 2000 modems connected to Cisco uBR10012 router (only Wideband Service offered), packets addressed to some customer premises equipment (CPEs) disappear. This occurs on a random card and a random IP address pool. Internet access fails in some random hosts.</p> <p>When a packet is sent from CPE to the remote system, the packet arrives and a response is sent but the CPE cannot receive it. Checking the downstream (DS) packet count for the specific modem shows no packet.</p> <p>Ping test from the Cisco uBR10012 router with any interface in it as source is successful but the same test from a PC to default gateway or any interface in the router fails. Ping test from the router to hosts is successful but the same test from DHCP server or other systems fails. When the PC powers up, it receives an IP address but cannot access internet. The <b>clear cable modem xxxx delete</b> command does not solve the problem at all times.</p> <p>Cable monitor captures incoming packets from hosts but cannot capture outgoing packets. There is there is MAC-IP information in ARP table in uBR10k and there is no problem in the ARP table in the PC.</p> <p>PRE switchover and system reboot do not resolve the problem.</p> <p>Conditions: This occurred when:</p> <ul style="list-style-type: none"> <li>• wideband modems were configured</li> <li>• Cisco IOS Release 12.3(21a)BC4 and only Cisco MC520H cards are installed</li> <li>• there was a 50MHz difference between channel 0 and 1</li> </ul> <p>Workaround: Clear IP ARP and get a new IP address.</p>
CSCso16183	<p>Symptom: SNMP may report different speeds and modulation types for upstream channels configured for the same type of modulation. The ifSpeed variable reported in SNMP conforms to 16QAM at 10.24Mbps on some interfaces but shows as QPSK at 5.12Mbps on others.</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running the Cisco IOS 12.3(23)BC3 with cable linecard interfaces configured for 16QAM (modulation profile 24) with the following configuration:</p> <ul style="list-style-type: none"> <li>• Spectrum-groups and upstream load balancing configured</li> <li>• Two upstream channels in the same US load balance group, and</li> <li>• Two upstreams in the same spectrum group.</li> </ul> <p>Workaround: There is no workaround.</p>
CSCsm44746	<p>Symptom: Potential array overflow.</p> <p>Condition: When cmts_cert_compliant flag is set to true.</p> <p>Workaround: There is no workaround.</p>
CSCso63567	<p>Symptom: When a cable modem is locked with primary channel from SPA, voice call tone dropout of 4500~5000ms was observed during bulk calls.</p> <p>Condition: Difficult to be recreated.</p> <p>Workaround: There is no workaround.</p>

**Table 31** Open Caveats for Cisco IOS Release 12.3(23)BC4 (continued)

DDTS ID Number	Description
CSCsr47518	<p>Symptom: The Cisco uBR10012 router reloads due to bus error.</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running Cisco IOS release 12.3(23)BC1 and later Cisco IOS releases.</p> <p>Workaround: There is no workaround.</p>
CSCso43883	<p>Symptom: The output of the <b>show tech-support</b> command contains SNMP community string passwords.</p> <p>Condition: This issue is observed when redundancy SNMP community string is configured.</p> <p>Workaround: There is no workaround.</p>
CSCso59182	<p>Symptom: Modems on a modular interface remain offline.</p> <p>Condition: This issue is observed when a remote DS channel is impaired and primary channel selection for bonded service is enabled using the following command:</p> <p><b>cable service attribute ds-bonded downstream-type bonding-enabled [enforce]</b></p> <p>Workaround: Check the remote channel operating condition and remove the impaired channel out of the mac domain configuration.</p>
CSCsr30738	<p>Symptom: SLOWRPC error message is generated in IPC code while booting the Cisco uBR10012 router.</p> <p>Workaround: There is no workaround.</p>
CSCso96838	<p>Symptom: Secondary PRE2 crashes.</p> <p>Condition: This issue is observed when the following exceptions are run:</p> <ul style="list-style-type: none"> <li>• no exception-slave core-file ubr3</li> <li>• no exception-slave dump 172.18.98.28</li> <li>• no exception core-file ubr3, and</li> <li>• no exception dump 172.18.98.28.</li> </ul> <p>Workaround: Do not remove the exception.</p>
CSCsq16982	<p>Symptom: Network interface on the Cisco uBR10012 router fails to acquire a global IPv6 address using IPv6 autoconfiguration command on the interface. IOS only supports SLAAC for autoconfiguration.</p> <p>Condition: This is a normal operation.</p> <p>Workaround: Configure a static IPv6 address on the interface.</p>
CSCek41611	<p>Symptom: Cisco MC5x20U linecards experience a silent reload. No crash information file is saved in the bootflash.</p> <p>Condition: Cisco uBR10012 router PRE-2 running Cisco IOS release 12.3(13a)BC2.</p> <p>Workaround: There is no workaround.</p>

**Table 31**      **Open Caveats for Cisco IOS Release 12.3(23)BC4 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsr07340	<p>Symptom: Backup TCC card may experience a reload (IPCOIR-3-TIMEOUT on TCC card).</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running Cisco IOS 12.3(23)BC1.</p> <p>Workaround: There is no workaround.</p>
CSCso60335	<p>Symptom: The <b>show hw-module all sensors</b> command does not show the desired output for Cisco uBR10012 router.</p> <p>Condition: This issue is observed in Cisco 12.2S based IOS releases.</p> <p>Workaround: Use alternate <b>show hw-module subslot all sensors</b> command for correct output.</p>
CSCsl92187	<p>Symptom: Change in syntax of cable modem remote-query command.</p> <p>Condition: This issue is observed when the no form of <b>cable modem remote-query</b> command changes the syntax.</p> <p>Workaround: There is no workaround.</p>
CSCsq35790	<p>Symptom: Voice over IP (VoIP) packets of Session Initiation Protocol (SIP) are not recognized. The VoIP packets are assigned to normal Committed Information Rate (CIR) queue instead of Low Latency Queuing (LLQ).</p> <p>Condition: This issue is observed when max ds latency information is not included in Dynamic Service Change (DSC) message.</p> <p>Workaround: Configure max ds latency information on cable modem.</p>
CSCsd14355	<p>Symptom: SNMP-created QoS profile is not available after a PRE switchover.</p> <p>Condition: The issue is observed when PRE switchover is performed after creating QoS profile using SNMP.</p> <p>Workaround: Use the command to create QoS profile instead of SNMP.</p>
CSCsq66453	<p>Symptom: Standby PRE fails on the Cisco uBR10012 router.</p> <p>Condition: Not known.</p> <p>Workaround: There is no workaround.</p>
CSCsm50955	<p>Symptom: A Cisco uBR10012 router with (N+1) linecards redundancy configured may log debug level tracebacks as the standby linecard is readying for switchover. No impact to traffic.</p> <pre>Feb 1 12:04:34.257: -Traceback= 6080D2DC 604A6D24 60797C44 6079DDC4 60453528 6079E81C 60798A84 6079938C Feb 1 12:04:34.257: DBG ERR: cr10k_docsis_hccp_get_req_buf get HCCP buf failed (207), type = 19, len = 4176</pre> <p>Condition: This issue is observed when information associated with a particular cable modem becomes too large and is prevented from being synchronized to the standby linecard.</p> <p>Workaround: There is no workaround.</p>

**Table 31** Open Caveats for Cisco IOS Release 12.3(23)BC4 (continued)

DDTS ID Number	Description
CSCsq23882	<p>Symptom: All cable linecards crash after a Cisco uBR10012 router PRE switchover.</p> <p>Condition: This issue is observed immediately after the PRE switchover.</p> <p>Workaround: There is no workaround.</p>
CSCsi94641	<p>Symptom: On a Cisco uBR10012 router, the wideband modems associated with the first SPA in bay 1/0/0 have their downstream service flow counters collated as expected, but wideband modems on 1/0/1 do not appear to show any wideband counters for downstream service flows.</p> <p>Condition: Wideband cable modems operating on the wideband SPA in the second jacket card bay. There is no problem with modems operating on the first SPA.</p> <p>Workaround: There is no workaround.</p>
CSCso92184	<p>Symptom: Wideband cable modems drop offline.</p> <p>Condition: None.</p> <p>Workaround: Connect all wideband cable modems onto the linecard(s) as "modular-host subslot".</p>
CSCs150048	<p>Symptom: Modems without minimum and maximum DS rate configured fail to register on modular-cable downstreams even when they use config files that have downstream llq (max downstream latency) set.</p> <p>Condition: These modems are stuck in reject(c) state.</p> <p>Workaround: Configure minimum and maximum DS rate in the downstream service flow encoding in the config file.</p>
CSCsm11169	<p>Symptom: High CPU utilization on Cisco 520X cable linecard during cable modem bringup.</p> <p>Conditions: When the Cisco uBR10012 router or a Cisco 520x cable linecard reloads, and there are numerous cable modems in the registration process.</p> <p>Workaround: There is no workaround.</p>
CSCsr46842	<p>Symptom: The wideband cable modems wrongly appear in the load balance exclude list besides appearing correctly in the load balance pending list.</p> <p>Workaround: There is no workaround.</p>
CSCso57024	<p>Symptom: The Cisco vendor-specific "Wideband Channel ID" option (vendor-specific option 14) does not work.</p> <p>Condition: This issue is observed when using a recent version of Scientific Atlanta wideband DPC2505 modem with the Cisco uBR10012 router.</p> <p>Workaround: There is no workaround.</p>

## Resolved Caveats for Release 12.3(23)BC4

Table 32 lists only severity 1 and 2 caveats and select severity 3 resolved caveats for Cisco IOS Release 12.3(23)BC4.

f

**Table 32 Resolved Caveats for Cisco IOS Release 12.3(23)BC4**

DDTS ID Number	Description
CSCsr56760	<p>Symptom: The <b>show diagnostic result subslot x/y detail</b> command displays incorrect <b>last test pass time</b> value.</p> <p>Conditions: On executing offline-field diagnostic tests, the last test pass time is the same as <b>last test execute time</b>.</p> <p>Workaround: Use the <b>show diagnostics events subslot x/y</b> command for the test pass time.</p>
CSCsq23758	<p>Symptom: US throughput drops by half after 12-18 minutes for wideband modems.</p> <p>Condition: This issue is observed on images using the Cisco IOS 12.3(23)BC.</p> <p>Workaround: Configure the CMTS without the shaping command.</p>
CSCsr78824	<p>Symptom: After deleting the <b>cable privacy accept-self-signed</b> setting and placing a manufacturer's self-signed certificate in the bootflash of the CMTS in a file named <b>root-cert</b> or <b>euro-root-cert</b>, the self-signed certificate appears to be loaded, but the devices still cannot come online(pt). The BPI+ negotiation fails.</p> <p>Condition: The affected devices cannot be used with both BPI+ and no accept-self-signed. Pre-configuring the certificate into the CMTS via either SNMP or command / configuration file also fails.</p> <p>Workaround: Provision a cable modem whose BPI+ certificate is not signed by a signing authority (eg: self-signed) when the CMTS is configured to reject self-signed certs. Load a copy of the manufacturer's certificate into the bootflash of the device.</p>
CSCso63578	<p>Symptom: A Cisco uBR10012 router running Cisco IOS release 12.3(23)BC3 may experience a memory leak in the Pool Manager. Use <b>show processes memory</b> to view memory status or use the ciscoMemoryPoolUsed MIB object.</p> <p>Condition: Mixture of best effort data traffic, UGS voice traffic and SNMP polling.</p> <p>Workaround: There is no workaround.</p>
CSCso61937	<p>Symptom: The Cisco uBR10-MC5X20U linecard fails due to memory corruption.</p> <p>Condition: This issue is observed while running Cisco IOS Release 12.3(23)BC1.</p> <p>Workaround: There is no workaround.</p>
CSCsr15208	<p>Symptom: Wideband SPA may not accept the SFP with serial number starting with AG.</p> <p>Condition: SFP has serial number starting with AG.</p> <p>Workaround: Run the <b>hw-module bay x/y/z reload</b> command.</p>

**Table 32** *Resolved Caveats for Cisco IOS Release 12.3(23)BC4 (continued)*

DDTS ID Number	Description
CSCsr93439	<p>Symptom: On reverting after a linecard switchover, some upstream cable modems go offline and do not return online because the PHY is in error state. Observed to occur with both, Cisco IOS Release 12.3(23)BC2 and Cisco IOS Release 12.3(23)BC3.</p> <p>Conditions: There are many upstream channels in no-shut state in the Cisco 520H linecard. This problem can occur on performing a switchover and reverting to the previous state.</p> <p>Workaround: Run the <b>shutdown/ no shutdown</b> command bring the cable modems online.</p>
CSCsr04644	<p>Symptom: Traceback observed after the following commands are run.</p> <ul style="list-style-type: none"> <li>• <b>cable dynamic-bw-sharing</b></li> <li>• <b>no shut</b></li> </ul> <p>Condition: The traceback is observed when an ARP entry in a bundle interface is to be deleted, or being created for the first time, with <b>debug cr10k_rp</b> on.</p> <p>Workaround: There is no workaround.</p>
CSCsr87364	<p>Symptom: On a Cisco uBR10000 series router, the CGD (downstream modular-cable) commands under the MAC Domain interface configuration disappear.</p> <p>Condition: Observed to occur after a cable linecard switchover followed by a PRE switchover.</p> <p>Workaround: Reverting the linecard to the working cable linecard would ensure that the commands are restored.</p>
CSCsu09572	<p>Symptom: On de-configuring or re-configuring HCCP, the flag <b>clc_cfg_done</b> in the standby PRE is not consistent with that in the active PRE. After PRE switchover the HCCP is in an incorrect state.</p> <p>Conditions: Observed after PRE bootup, de-configuring and re-configuring HCCP on active PRE.</p> <p>Workaround: Reset the standby PRE.</p>

## Open Caveats for Release 12.3(21a)BC8

Table 33 lists only severity 1 and 2 caveats and select severity 3 open caveats for Cisco IOS Release 12.3(21a)BC8.

**Table 33**      **Open Caveats for Cisco IOS Release 12.3(21a)BC8**

DDTS ID Number	Description
CSCsr75525	<p>Symptom: Incorrect power values for Power Entry Modules (PEM) displayed by the <b>show controllers clock-reference</b> command.</p> <p>While PEM0 + PEM1 should not be higher than 2400, a single PEM's power exceeds that value.</p> <p>Conditions: Cisco uBR10012 TCC card is used.</p> <p>Workaround: There is no workaround. Cisco uBR10012 TCC reseating does not solve the problem.</p>
CSCsl72140	<p>Symptom: Cable modems get stuck in init(io) because they cannot receive DHCP Offer and cannot proceed further.</p> <p>Conditions: This occurs occasionally on some modems.</p> <p>Workaround: Change the MAC address of the PC and get a new IP address using the <b>clear cable modem [mac-address] delete</b> command.</p>
CSCso87178	<p>Symptom: Modems in random upstream(US) ports go offline and return to online status in a few minutes. This is recorded and displayed as output of the <b>show cable flap-list</b> command.</p> <p>Conditions: This has been reported from newly installed Cisco uBR10012 Routers having Cisco MC520H linecard.</p> <p>Workaround: Wait for a few minutes for automatic correction.</p>
CSCsm47906	<p>Symptom: Modems go offline after a severe noise in the Hybrid Fiber-Coaxial (HFC) end.</p> <p>Conditions: Severe Noise on the HFC with pre-equalization enabled.</p> <p>Workaround: Disable pre-equalization using the <b>no cable upstream 0 equalization-coefficient</b> command.</p>

Table 33 Open Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)

DDTS ID Number	Description
CSCsm12010	<p>Symptoms: With about 2000 modems connected to Cisco uBR10012 router (only Wideband Service offered), packets addressed to some customer premises equipment (CPEs) disappear. This occurs on a random card and a random IP address pool. Internet access fails in some random hosts.</p> <p>When a packet is sent from CPE to the remote system, the packet arrives and a response is sent but the CPE cannot receive it. Checking the downstream (DS) packet count for the specific modem shows no packet.</p> <p>Ping test from the Cisco uBR10012 router with any interface in it as source is successful but the same test from a PC to default gateway or any interface in the router fails. Ping test from the router to hosts is successful but the same test from DHCP server or other systems fails. When the PC powers up, it receives an IP address but cannot access internet. The <b>clear cable modem xxxx del</b> command does not solve the problem at all times.</p> <p>Cable monitor captures incoming packets from hosts but cannot capture outgoing packets. There is there is MAC-IP information in ARP table inubr10k and there is no problem in the ARP table in the PC.</p> <p>PRE switchover and system reboot do not resolve the problem.</p> <p>About 10 CPEs report this error per day.</p> <p>Conditions: This occurred when:</p> <ul style="list-style-type: none"> <li>• wideband modems were configured</li> <li>• Cisco IOS Release12.3(21a)BC4 and only Cisco MC520H cards are installed</li> <li>• there was a 50MHz difference between channel 0 and 1</li> </ul> <p>Workaround: Clear IP ARP and get a new IP address.</p>
CSCso63567	<p>Symptom: When a cable modem is locked with primary channel from SPA, voice call tone dropout of 4500~5000ms was observed during bulk calls.</p> <p>Condition: Difficult to be recreated.</p> <p>Workaround: There is no workaround.</p>
CSCek41611	<p>Symptom: Cisco MC5x20U linecards experience a silent reload. No crash info file is saved in the bootflash.</p> <p>Condition: Cisco uBR10012 router PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>Workaround: There is no workaround.</p>
CSCsq35790	<p>Symptom: Voice over IP (VoIP) packets of Session Initiation Protocol (SIP) are not recognized. The packets have to be assigned to normal Committed Information Rate (CIR) queue instead of Low Latency Queuing (LLQ).</p> <p>Conditions: Not including Max Downstream Latency information in Dynamic Service Change (DSC) message.</p> <p>Workaround: On a cable modem, Max Downstream Latency information has to be configured.</p>

**Table 33** *Open Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)*

DDTS ID Number	Description
CSCsr70184	Symptom: Access to a gate is refused due to exceeded activity-count even when the subscriber has no gate assigned. Conditions: Packetcable was running. Workaround: Increase the activity count in the gate set message.
CSCsm11169	Symptom: High CPU utilization on Cisco 520x cable linecard during cable modem bringup. Conditions: When the Cisco uBR10012 router or a Cisco 520x cable linecard reloads, and there are numerous cable modems in the registration process. Workaround: There is no workaround.

## Resolved Caveats for Release 12.3(21a)BC8

Table 34 lists only severity 1 and 2 caveats and select severity 3 resolved caveats for Cisco IOS Release 12.3(21a)BC8.

**Table 34** *Resolved Caveats for Cisco IOS Release 12.3(21a)BC8*

DDTS ID Number	Description
CSCso42612	Symptom: The SNMP response is slow when ccwbWBCmStatusValue is polled on the Cisco uBR10012 router. Workaround: There is no workaround.
CSCsk65431	Symptom: Changing IP address on the int bundle X.1 subinterface results in an Integrated Upconverter flap for all interfaces associated with that bundle. Condition: This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17)BC or higher that has a bundle interface configured. Workaround: There is no workaround.
CSCsq79058	Symptom: Unable to set the MIB objects "ccwbRFChanQamIPAddress", "ccwbRFChanQamMacAddress" and "ccwbRFChanQamUdpPort" separately. Workaround: Set the MIB objects "ccwbRFChanQamIPAddress", "ccwbRFChanQamMacAddress" and "ccwbRFChanQamUdpPort" in single instruction set.
CSCsq53782	Symptom: A false INFO level alarm is raised when using non-default configuration for "max-ports" and "connector" on upstream port, even when the port is actually up and running. Workaround: There is no workaround.
CSCsq47785	Symptom: The secondary PRE serial number of the Cisco uBR10012 router is shown as "N/A". Workaround: Use <b>show diag</b> command to display the serial number.

Table 34 Resolved Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)

DDTS ID Number	Description
CSCso78689	<p>Symptom: When an interface, usually a line card (Gigabit Ethernet), with an output service policy with random detect is removed, an assertion failure results. These assertion messages are logged every 10 seconds.</p> <p>Condition: This issue is observed if an interface with an output service policy with random detect is removed (commonly the result of removing a line card).</p> <p>Workaround: Remove the output service policy from the interface prior to removal of the line card.</p>
CSCs142554	<p>Symptom: All cable modems go offline with no alert or log message. When <b>clear cable modem all delete</b> command was executed, no CM was ranging. When checked, upconverter signal was ok and ucd counter also normal.</p> <p>Condition: This issue is observed in routers with the Cisco MC520H linecard.</p> <p>Workaround: Use <b>cable downstream rf-shutdown</b> and <b>no cable downstream rf-shutdown</b> commands.</p>
CSCso42653	<p>Symptom: During installation of a new chassis with the DTCC card, when modems are moved from the old chassis to the new one, some of the modems do not come online and are stuck in the init(rc) state. Pre-equalization control on the cable modems is also not enabled.</p> <p>Workaround: Change the upstream modulation to the Quadrature Phase-Shift Keying (QPSK) modulation.</p>
CSCso04521	<p>Symptom: The Cisco uBR10012 router may crash when executing the <b>test cable load-balance ucc</b> command.</p> <p>Workaround: There is no workaround.</p>
CSCsm55512	<p>Symptom: Tracebacks occur every time when INVALIDSIDPOSITION error is displayed in a CMTS that has a large number of cable modems with a few going offline.</p> <p>Workaround: There is no workaround.</p>
CSCs187023	<p>Symptom: The <b>Running-configuration</b> and <b>show controllers</b> commands show different output values for upstream center frequency.</p> <p>Condition: This is found when the fixed upstream center frequency is configured.</p> <p>Workaround: There is no workaround.</p>
CSCsg61902	<p>Symptoms:</p> <ol style="list-style-type: none"> <li>1. Duplicate system log messages and local log messages are observed for LINK UP of cable interface.</li> <li>2. HCCP revert-back raised minor alarms for every downstream ports on the protect CLC if the <b>shutdown</b> and <b>no shutdown</b> commands are run on the cable interfaces on the protect cable linecard before reverting.</li> </ol> <p>Workaround: The workarounds for the symptoms mentioned above are numerically described below.</p> <ol style="list-style-type: none"> <li>1. None</li> <li>2. Run <b>shutdown</b> and <b>no shutdown</b> commands to clear the minors alarms in the cable interfaces.</li> </ol>

**Table 34** *Resolved Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)*

DDTS ID Number	Description
CSCsm46631	<p>Symptom: There are discrepancies in the outputs of <b>show diag</b> and <b>show inventory</b> commands for the Cisco 520U and 520H cable interface linecards. The mismatch occurs in PID, SN and VID values of the output.</p> <p>Condition: The issue is found on routers running Cisco IOS Release 12.3(21a)BC4 and later Cisco IOS releases.</p> <p>Workaround: There is no workaround.</p>
CSCsj56668	<p>Symptom: The actual number of CPEs allowed is greater than the maximum CPE value that is configured in the cable modem verbose.</p> <p>Conditions: This problem is found when the max CPE value is configured in the interface configuration mode.</p> <p>Workaround: There is no workaround.</p>
CSCsg91306	<p>Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.</p> <p>Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.</p> <p>There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip</a></p>
CSCsk42759	<p>Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.</p> <p>Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.</p> <p>There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip</a></p>

**Table 34 Resolved Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)**

DDTS ID Number	Description
CSCso76704	<p>Symptom: While performing PRE2 switchover, the following errors were displayed:</p> <pre>F241-38-03-UBR10K-1#redundancy force-failover main-cpu Proceed with switchover to standby PRE? [confirm]y % HCCP 1 50 Switchover in progress. HA system in transient state, switchover aborted.</pre> <p>One of the reason is that one of the cable linecard is locked out. It should indicate it is a lockout instead of switchover.</p> <p>Condition: When one or more cable linecard is locked out, the PRE2 switchover gives misleading message.</p> <p>Workaround: Run <b>show hccp detail   include lockout</b> command before PRE2 switchover.</p>
CSCek79183	<p>Symptom: The following message and traceback are seen with a uBR10012 router running the Cisco IOS 12.3(21a)BC4 release indicating the IPC timeout between the working and protect linecard.</p> <pre>SLOT 8/1: Jul 19 03:23:08.643 PDT: %REQGRP-3-SYSCALL: System call for command 10 (slot5/1) : Nonblocking request failed (Cause: timeout) -Traceback= 604DC7C0 604F78F4 604F9EFC 604FA59C 604FAD90</pre> <p>Condition: The message and traceback are seen after upgrading the IOS to 12.3(21a)BC4 version.</p> <p>Workaround: There is no workaround.</p>
CSCso76808	<p>Symptom: Primary downstream service flow with non-zero DOCSIS priority appears to get synced to the standby PRE with priority set to zero. This results in the corresponding queues being created on the standby PRE prior to switchover with incorrect parameters.</p> <p>Condition: Set downstream priority in the cable modem config file.</p> <p>Workaround: There is no workaround.</p>
CSCso38313	<p>Symptom: On a Cisco uBR10012 router , the active PRE2 crashes and failover to standby PRE occurs when the Protect linecard is in active state.</p> <p>Condition: This is observed on a uBR10012 router running Cisco IOS Release 12.3(17b)BC4 and configured for global N+1 linecard redundancy (HCCP).</p> <p>Workaround: There is no workaround.</p>
CSCso82323	<p>Symptom: The primary PRE crashes after PRE switchover.</p> <p>Condition: This issue is observed when the following steps are performed with LC5/1 linecard acting as protect and LC7/0 as working.</p> <ol style="list-style-type: none"> <li>1. Switchover from 7/0 to 5/1.</li> <li>2. Shutdown one of active protect interface, such as 5/1/2.</li> <li>3. Revert to 7/0 using <b>redundancy linecard revertback 7/0</b> command.</li> <li>4. Do a PRE switchover using <b>redundancy force-failover main-cpu</b> command.</li> <li>5. Perform the <b>no shutdown 5/1/2</b> command resulting in crash in new active PRE.</li> </ol> <p>Workaround: Do not shutdown the linecard interface acting as protect.</p>

**Table 34** Resolved Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)

DDTS ID Number	Description
CSCso86994	<p>Symptom: The standby Cisco uBR10012 router PRE crashes.</p> <p>Condition: This issue is observed when the following steps are performed with LC5/1 linecard acting as protect and LC7/0 as working.</p> <ol style="list-style-type: none"> <li>1. Switchover from 7/0 to 5/1.</li> <li>2. Shutdown one of active protect interface, such as 5/1/2.</li> <li>3. Boot up standby PRE.</li> <li>4. Run the <b>no shutdown</b> 5/1/2 command.</li> <li>5. Revert to 7/0 using <b>redundancy linecard revertback 7/0</b> command. This command causes crash in standby PRE.</li> </ol> <p>Workaround: Do not shutdown the linecard interface acting as protect.</p>
CSCsq02262	<p>Symptom: Based on the HCCP design, IPC timeout should trigger the linecard switchover. However, the IPC timeout does not trigger the linecard switchover but only shuts down the specific interface.</p> <p>Workaround: There is no workaround.</p>
CSCsq19079	<p>Symptom: Running configuration details of PRE modules becomes inconsistent after a PRE switchover.</p> <p>Condition: This issue is observed when the following steps are performed:</p> <ol style="list-style-type: none"> <li>1. Working linecard failover to protect linecard.</li> <li>2. Shutdown the w linecard.</li> <li>3. Do a PRE switchover.</li> </ol> <p>Workaround: There is no workaround.</p>
CSCso08115	<p>Symptom: The HCCP sync-pulse logic can lead to unexpected resets and/or switchovers of working linecards due to defective protect linecards.</p> <p>Workaround: There is no workaround.</p>
CSCsq50907	<p>Symptom: When an HCCP switchover is done, one of the upstream channels on each frequency stacked ports lose communication to the modems connected to it.</p> <p>Condition: The <b>show controller</b> command output does not show the upstream port assignments for the affected upstream channels.</p> <p>This issue is observed on a Cisco uBR10012 router running Cisco IOS 12.3(23)BC2 release.</p> <p>Workaround: There is no workaround.</p>
CSCsr45093	<p>Symptom: Protect interfaces are protecting two different working linecards at the same time.</p> <p>Conditions: This issue occurs when some standby interfaces are shut down and some cards are out of service (crash, power off, etc).</p> <p>Workaround: Use <b>no shutdown</b> command at the working interface and revert from protect card to working card.</p>

**Table 34 Resolved Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)**

DDTS ID Number	Description
CSCso61633	<p>Symptom: The Cisco uBR10012 router with PRE2 becomes at cmts_hccp_load_config.</p> <p>Condition: This is observed on the router running Cisco IOS Release 12.3(23)BC1 and later Cisco IOS releases.</p> <p>Workaround: There is no workaround.</p>
CSCso73405	<p>Symptom: Traceback was observed on both active and standby RPs.</p> <p>Condition: Linecard switchover during PRE bulk sync.</p> <p>Workaround: Do not perform linecard failover until standby RP reach Standby_Hot state (for SSO mode) or Standby_Cold state (RPR mode).</p>
CSCso74192	<p>Symptom: The <b>show cable clock</b> command returned incorrect value for number of TCC cards.</p> <p>Condition: Insert new DTCC cards into slot 1/1 and 2/1 and do a PRE2 switchover.</p> <p>Workaround: Perform another PRE2 switchover.</p>
CSCek52673	<p>Symptom: DHCP server-enabled router is reloading after receiving a malformed UDP packet.</p> <p>Condition: Load the router with default config and run the following linux command: <code>udpsic -s rand -d 2.2.2.2,67 -r 26230 -k 2 -p 3</code></p> <p>Workaround: There is no workaround.</p>
CSCsr05759	<p>Symptom: If the cable modem is rebooted, the CMTS forwards its DHCP Discover through a different VRF than expected. However, the subsequent DHCP Request is sent through the correct VRF so that it cannot be correlated to the DHCP Offer.</p> <p>Condition: This issue occurs when multiple bundle interfaces having unique VRFs are associated with the same downstream.</p> <p>Workaround: Either terminate VRFs on a single DHCP server ignoring VRF values, or keep clearing the CMs with a script.</p>
CSCso79280	<p>Symptom: A Cisco uBR10012 router with the Cisco UBR10-MC5X20 linecard may fail due to excessive memory allocation failures with low memory errors.</p> <p>Condition: This is observed on the router running Cisco IOS Release 12.3(21a)BC4 with ESR-PRE2 module.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Perform the online insertion and removal (OIR) process on the linecard. OIR instructions can be found at:  <a href="http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_linecard_oir_ps2209_TSD_Products_Configuration_Guide_Chapter.html">http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_linecard_oir_ps2209_TSD_Products_Configuration_Guide_Chapter.html</a></li> <li>2. Reset the Hw-module subslot 5/1.</li> </ol>

**Table 34** Resolved Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)

DDTS ID Number	Description
CSCsq72700	<p>Symptom: If DSA or DSC-Req is sent by the Embedded Media Terminal Adapter (eMTA) with DOCSIS Nominal Grant Interval set to 0, then cable linecard would crash.</p> <p>Condition: This issue occurs when eMTA with DOCSIS Nominal Grant Interval for a UGS-AD service flow is set to 0.</p> <p>Workaround: Turn off silence suppression.</p>
CSCsj40978	<p>Symptom: The Cisco uBR10012 router fails to boot or fails when a request for BPI+ session is received.</p> <p>Condition: This issue is observed when the US and EU root certificates are not present on the file system.</p> <p>Workaround: Ensure that the US and EU certificates are present in the file system before security is enabled.</p>
CSCsg50812	<p>Symptom: Multicast traffic is dropped by the Half Height Gigabit Ethernet (HHGE) or Full Height Gigabit Ethernet (FHGE) linecards when links of an EtherChannel port are bounced by the <b>shutdown</b> or <b>no shutdown</b> command causing the OSPF neighbor not going into full state.</p> <p>Workaround: Use the <b>shutdown</b> or <b>no shutdown</b> command at the aggregate Ethernet Channel port.</p>
CSCsg81770	<p>Symptom: A subinterface with ifIndex=62 does not show up in the IFMIB output.</p> <p>Condition: When the router is configured such that the ifIndex value of 62 gets assigned to a subinterface (non-HWIDB), the interface may not show up in the IFMIB output.</p> <p>Workaround: Enable ifIndex persistence using the <b>snmp ifindex persist</b> command when ifIndex 62 is given to a HWIDB. Or configure the router's interfaces in such a way that ifIndex 62 is given to a HWIDB.</p> <p> <b>Note</b> You will need to reload the Cisco uBR10012 router if this condition is encountered.</p>
CSCsm77199	<p>Symptom: If the HTTP secure server capability is present, the switch shows the following error message:</p> <pre>%DATACORRUPTION-1-DATAINCONSISTENCY:</pre> <p>Condition: This issue occurs if the HTTP server is configured using the <b>ip http server</b> command.</p> <p>Workaround: Disable the HTTP server using the <b>no ip http server</b> command.</p> <p> <b>Note</b> The switch functionality is not affected by this error message.</p>
CSCsj46707	<p>Symptom: The Cisco uBR10012 router hangs during bootup.</p> <p>Condition: The router usually hangs during a race condition.</p> <p>Workaround: There is no workaround.</p>

**Table 34** *Resolved Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsq05652	<p>Symptom: Incorrect display of active calls when nRTPS or RTPS is configured.</p> <p>Condition: The RTPS or nRTPS is interpreted as a call in the output of the <b>show cable calls</b> and <b>show cable modem calls</b> commands.</p> <p>Workaround: Use <b>show packetcable gate summary</b> command to check the status of active calls.</p>
CSCsm52934	<p>Symptom: The previously disabled JIB upstream port becomes enabled after the Cisco uBR10-MC5X20U linecard is reset.</p> <p>Workaround: Run the <b>shut</b> and <b>no shut cable interface</b> commands to correct the anomaly.</p>
CSCsj10923	<p>Symptom: Issuing a <b>shut</b> or <b>no shut</b> command on the protect interface causes the interface on the working card to become active.</p> <p>Condition: This error occurs if you issue the command when the protect interface is active.</p> <p>Workaround: Do not issue the <b>shut</b> or <b>no shut</b> command on the protect interface, which is active.</p>
CSCsq66130	<p>Symptom: Flowbits keep asserting after an OIR is performed on a SPA, and a traceback is also observed when the <b>show pxf cpu queue</b> command is used.</p> <p>Condition: This problem is observed with the SPA OIR.</p> <p>Workaround: There is no workaround.</p>
CSCsr03421	<p>Symptom: The standby PRE crashes when a linecard has more than 512 ongoing calls.</p> <p>Condition: This issue occurs if two gates with the same offset are on the free gate list.</p> <p>Workaround: Remove the standby PRE.</p>
CSCsq37824	<p>Symptom: Memory over flow is observed.</p> <p>Workaround: There is no workaround.</p>
CSCsr23126	<p>Symptom: Upstream load balancing breaks with DOCSIS 3.0 certified modems in a w-online(pt) state.</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running Cisco IOS Release 12.3(21a)BC.</p> <p>Workaround: There is no workaround.</p>
CSCsj58093	<p>Symptom: CPE ping stops after the wideband (WB) switches to the narrowband (NB) mode.</p> <p>Condition: This problem occurs when you shut down the WB interface.</p> <p>Workaround: Execute <b>clear arp</b> or <b>clear cable modem</b> commands to clear the ARP entries and then let the cable modem on the NB to come online.</p>
CSCsh69471	<p>Symptom: AAA accounting requests are being sent with empty user name.</p> <p>Condition: This issue occurs while running the <b>show accounting</b> command for the affected accounting traffic.</p> <p>Workaround: No workaround is required as it is only a display issue.</p>

**Table 34** Resolved Caveats for Cisco IOS Release 12.3(21a)BC8 (continued)

DDTS ID Number	Description
CSCsj12495	<p>Symptom: In a high availability configuration with multiple PREs, the standby PRE might reload when a new line card is inserted.</p> <p>Condition: This issue occurs when inserting a new line card in the chassis.</p> <p>Workaround: There is no workaround.</p>
CSCsk60014	<p>Symptom: No downstream throughput for PC calls on eMTA accompanied by a warning after a PRE failover. The problem occurs because the standby PRE fails to start its WBCMTS periodic timer after the failover. When the problem occurs wideband capable modems fail to come online in wideband mode and register as narrowband modems instead.</p> <p>Condition: The problem occurs if the failover happens before the Wideband SPA has reached its operational state. This could happen if the card was not inserted prior to the failover. This could also happen if the failover occurred concurrently with downloading the operational firmware. For example, it could happen if the active and standby PREs boot simultaneously and the active PRE is in the process of bringing up the WB SPA when a PRE failover occurs.</p> <p>Workaround: Reload the router.</p>
CSCso84029	<p>Symptom: Upstream traffic is not controlled according to the the penalty enforce class in CMTS routers, when the CM is penalized.</p> <p>Condition: When a CM is a penalized and associated with the penalty service class, US traffic is allowed to exceed the penalty class.</p> <p>Workaround: There is no workaround.</p>
CSCsq84686	<p>Symptom: All modems on a given upstream may go offline.</p> <p>Workaround: Run the <b>shutdown/no shutdown</b> commands on the cable upstream interface:</p> <ol style="list-style-type: none"> <li>1. cable upstream shutdown</li> <li>2. no cable upstream shutdown</li> </ol>

## Open Caveats for Release 12.3(23)BC3

Table 35 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(23)BC3.

**Table 35**      **Open Caveats for Cisco IOS Release 12.3(23)BC3**

DDTS ID Number	Description
CSCso16183	<p>Symptom: SNMP may report different speeds and modulation types for upstream channels configured for the same type of modulation. The ifSpeed variable reported in SNMP conforms to 16QAM at 10.24Mbps on some interfaces but shows as QPSK at 5.12Mbps on others.</p> <p>Condition: This issue is observed on a Cisco uBR10012 running 12.3(23)BC3 with cable linecard interfaces configured for 16QAM (modulation profile 24) with the following configuration:</p> <ul style="list-style-type: none"> <li>• Spectrum-groups and upstream load balancing configured</li> <li>• Two upstream channels in the same US load balance group, and</li> <li>• Two upstreams in the same spectrum group.</li> </ul> <p>Workaround: There are no known workarounds.</p>
CSCsd14355	<p>Symptom: SNMP created QOS profile is not available after a PRE switchover.</p> <p>Condition: The issue is observed when PRE switchover is performed after creating QOS profile using SNMP.</p> <p>Workaround: Use CLI to create QOS profile instead of SNMP.</p>
CSCsm44746	<p>Symptom: Potential array overflow.</p> <p>Condition: When cmts_cert_compliant flag is set to true.</p> <p>Workaround: There are no known workarounds.</p>
CSCsi94641	<p>Symptom: On a Cisco uBR10012 router, the wideband modems associated with the first SPA in bay 1/0/0 have their downstream service flow counters collated as expected, but wideband modems on 1/0/1 do not appear to show any wideband counters for downstream service flows.</p> <p>Condition: Wideband cable modems operating on the wideband SPA in the second jacket card bay. There is no problem with modems operating on the first SPA.</p> <p>Workaround: There is no workaround.</p>
CSCso63578	<p>Symptom: A Cisco uBR10012 router running 12.3(23)BC3 may experience a memory leak in the Pool Manager. Use <b>show processes memory</b> to view memory status or use the ciscoMemoryPoolUsed MIB object.</p> <p>Condition: Mixture of best effort data traffic, UGS voice traffic and SNMP polling.</p> <p>Workaround: There are no known workarounds.</p>

**Table 35** *Open Caveats for Cisco IOS Release 12.3(23)BC3 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCso82923	<p>Symptom: The cable interface configuration <b>cable dci-upstream-disable &lt;mac-address&gt; [enable disable]</b> appears to have no affect on the configuration.</p> <p>Condition: The MAC message is optional for modems, many modems ignore the MAC message.</p> <p>Workaround: Provision the cable modem with:</p> <ul style="list-style-type: none"> <li>• A DOCSIS 1.1 QOS profile of 10 Kbps upstream + 10kbps downstream</li> <li>• BPI + enabled, and</li> <li>• PC access denied.</li> </ul> <p>Do not use a max-cpe of 0 (unlimited CPE), use a max-cpe of 1.</p>
CSCsq23758	<p>Symptom: US throughput drops by half after 12-18 minutes for WB modems.</p> <p>Condition: This issue is observed on images using 12.3(23)BC.</p> <p>Workaround: Configure the CMTS without the shaping command.</p>
CSCso92184	<p>Symptom: Wideband cable modems drop offline.</p> <p>Condition: None.</p> <p>Workaround: Connect all wideband cable modems onto the linecard(s) as "modular-host subslot".</p>
CSCso87178	<p>Symptom: For newly installed two Cisco uBR10012 routers, modems drops offline in random US port.</p> <p>Condition: This issue is observed in Cisco uBR10-MC5X20H card only.</p> <p>Workaround: Wait for 5-8 minutes for modems to get online again.</p>
CSCso56190	<p>Symptom: The <b>show cable fiber-node</b> command does not display the description line entered under the fiber node in the running configuration.</p> <p>Condition: This issue is observed with following configuration:</p> <pre>R7508-uBR10K#sh cable fiber Fiber-Node 1   Local Primary Channels:   Remote RF Channels:     SPA 1/0/0: 0-3   FN Config Status: Configured (status flags = 0x1)   MDD Status: Valid  R7508-uBR10K#sh run   beg fiber-node cable fiber-node 1   description ALL DS on EQAM   downstream Modular-Cable 1/0/0 rf-channel 0-3   upstream Cable 5/0 connector 0</pre> <p>Workaround: Run the <b>show run   beg fiber-node</b> command.</p>
CSCsr47518	<p>Symptom: Cisco Router reloads due to bus error.</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC1 and later.</p> <p>Workaround: There are no known workarounds.</p>

**Table 35**      **Open Caveats for Cisco IOS Release 12.3(23)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCso43883	<p>Symptom: The output of the <b>show tech-support</b> commands contains snmp community string passwords.</p> <p>Condition: This issue is observed when redundancy SNMP community string is configured.</p> <p>Workaround: There are no known workarounds.</p>
CSCsk50223	<p>Symptom: The downstream modems failed to sync with the CMTS.</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running Cisco IOS code 12.3(13a)BC6 or Cisco IOS code 12.3(23)BC3 and Cisco uBR10-MC5X20U-D linecard.</p> <p>Workaround: Power off/on the Cisco uBR10-MC5X20U-D card.</p>
CSCso59182	<p>Symptom: Modems on a modular interface remain offline.</p> <p>Condition: This issue is observed when a remote DS channel is impaired and primary channel selection for bonded service is enabled using the following CLI command:</p> <pre>cable service attribute ds-bonded downstream-type bonding-enabled [enforce]</pre> <p>Workaround: Check the remote channel operating condition and remove the impaired channel out of the mac domain configuration.</p>
CSCs150048	<p>Symptom: Modems without minimum and maximum DS rate configured fail to register on modular-cable downstreams even when they use config files that have downstream llq (max downstream latency) set.</p> <p>Condition: These modems are stuck in reject(c) state.</p> <p>Workaround: Configure minimum and maximum DS rate in the downstream service flow encoding in the config file.</p>
CSCso63105	<p>Symptom: STM rate-limited traffic may exceed the limit.</p> <p>Condition: This issue is observed when rate-adapt is configured and flow is rate-adapt enabled.</p> <p>Workaround: Disable rate-adapt or change rate-adapt configuration such that flows that are eligible for STM are not eligible for rate-adapt.</p>
CSCsr15208	<p>Symptom: Wideband SPA may not accept the SFP with serial number starting with AG.</p> <p>Condition: SFP has serial number starting with AG.</p> <p>Workaround: Perform <b>hw-module bay x/y/z reload</b>.</p>
CSCsr30738	<p>Symptom: SLOWRPC error message is generated in IPC code while booting Cisco uBR10012 router.</p> <p>Workaround: There are no known workarounds.</p>

**Table 35** *Open Caveats for Cisco IOS Release 12.3(23)BC3 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsr52709	<p>Symptom: Service flow counts are not updated for downstream service flows handled by the 24 rfchannel SPA. As a result dynamic service flows for voice may be torn down when the T8 (inactivity) timer expires.</p> <p>Condition: This issue is observed when SPA in Bay 0 is inserted but the GigE link is disconnected or offline.</p> <p>Workaround: Ensure that the SPA0 GigE link is up whenever SPA 0 exists.</p>
CSCsl80817	<p>Symptom: The Packets per second (pps) rate for a voice call is always less than 49 pps.</p> <p>Condition: Due to data traffic saturation in both upstream and downstream directions, the voice call pps is reduced to less than 49 pps.</p> <p>Workaround: There are no known workarounds.</p>
CSCsq66453	<p>Symptom: Standby PRE crashes on Cisco uBR10012 router.</p> <p>Condition: Not known.</p> <p>Workaround: There are no known workarounds.</p>
CSCsm50955	<p>Symptom: A Cisco uBR10012 with N+1 Line Cards redundancy configured may log debug level tracebacks as the standby linecard is readying for switchover. No impact to traffic.</p> <pre>Feb 1 12:04:34.257: -Traceback= 6080D2DC 604A6D24 60797C44 6079DDC4 60453528 6079E81C 60798A84 6079938C Feb 1 12:04:34.257: DBG ERR: cr10k_docsis_hccp_get_req_buf get HCCP buf failed (207), type = 19, len = 4176</pre> <p>Condition: This issue is observed when information associated with a particular cable modem becomes too large and is prevented from being synchronized to the standby linecard.</p> <p>Workaround: There are no known workarounds.</p>
CSCsq23882	<p>Symptom: All cable line cards crash after a Cisco uBR10012 router PRE switchover.</p> <p>Condition: This issue is observed immediately after the PRE switchover.</p> <p>Workaround: There are no known workarounds.</p>
CSCsq89541	<p>Symptom: The Cisco uBR10012 router with PRE2 may cause on-net and off-net call rejection by CMTS due to GATE SET ERR and PKTCBL ERROR.</p> <p>Condition: This issue is observed when PRE2 is running on Cisco IOS 12.3(23)BC1 in PacketCable environment.</p> <p>Workaround: There are no known workarounds.</p>
CSCsl72140	<p>Symptom: Few wideband cable modems, with similar configurations, were stuck in the <b>init(io)</b> state and could not proceed further.</p> <p>Condition: No particular condition known.</p> <p>Workaround: Execute <b>clear cable modem [mac-address] delete</b> command.</p>

Table 35 Open Caveats for Cisco IOS Release 12.3(23)BC3 (continued)

DDTS ID Number	Description
CSCsm12010	<p>Symptom: In a uBR10012 router, packets sent from the cable modems to some Customer Premise Equipments (CPE) are lost due to possible hardware ARP information.</p> <p>Condition: This is observed when 2000 or more wideband modems are connected to a uBR10012 router.</p> <p>Workaround: Run <b>clear ip arp &lt;mac-address&gt;</b> command to get a new IP address.</p>
CSCso96838	<p>Symptom: Secondary PRE2 crashes.</p> <p>Condition: This issue is observed when the following exceptions are run:</p> <ul style="list-style-type: none"> <li>• no exception-slave core-file ubr3</li> <li>• no exception-slave dump 172.18.98.28</li> <li>• no exception core-file ubr3, and</li> <li>• no exception dump 172.18.98.28.</li> </ul> <p>Workaround: Do not remove the exception.</p>
CSCsq16982	<p>Symptom: Network interface on the Cisco uBR10012 CMTS fails to acquire a global IPv6 address using IPv6 autoconfiguration CLI on the interface. IOS only supports SLAAC for autoconfiguration.</p> <p>Condition: This is a normal operation.</p> <p>Workaround: Configure a static IPv6 address on the interface.</p>
CSCek41611	<p>Symptom: The MC5x20U linecards experience a silent reload.</p> <p>Condition: This issue is observed on a PRE-2 running Cisco IOS 12.3(13a)BC2 and later Cisco IOS releases.</p> <p>Workaround: There are no known workarounds.</p>
CSCsm47906	<p>Symptom: Cable modems drop offline.</p> <p>Condition: This issue is observed when:</p> <ul style="list-style-type: none"> <li>• A severe noise is found on the hybrid fiber-coaxial (HFC) system.</li> <li>• Pre-equalization is enabled.</li> </ul> <p>Workaround: Disable and re-enable pre-equalization. In other words, execute:</p> <pre>no cable upstream 0 equalization-coefficient cable upstream 0 equalization-coefficient</pre>
CSCsr07340	<p>Symptom: Backup TCC card may experience a reload (IPCOIR-3-TIMEOUT on TCC card).</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running Cisco IOS 12.3(23)BC1.</p> <p>Workaround: There are no known workarounds.</p>

**Table 35** *Open Caveats for Cisco IOS Release 12.3(23)BC3 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsr09380	<p>Symptom: Some modems fail to reach online(pt) state after a CMTS power cycle.</p> <p>Condition: If the hardware clock of the CMTS is set incorrectly, which may be outside the valid dates for the DOCSIS root certificate or EuroDOCSIS root certificate, the required / expected behavior is to reject all modems.</p> <p>Workaround: Correctly set the hardware clock on the processor card using the following commands:</p> <ul style="list-style-type: none"> <li>• <b>show clock</b></li> <li>• <b>set clock</b></li> <li>• <b>clock update-calendar</b></li> </ul> <p>Verify that the clock is properly set on the secondary PRE via the secondary PRE console.</p>
CSCso60335	<p>Symptom: The <b>show hw-module all sensors</b> command does not show any output for Cisco uBR10012 router.</p> <p>Condition: This issue is observed in Cisco 12.2S based IOS releases.</p> <p>Workaround: Use alternate command <b>show hw-module subslot all sensors</b> for correct output.</p>
CSCso61937	<p>Symptom: The Cisco uBR10-MC5X20U line card crashes due to memory corruption.</p> <p>Condition: This issue is observed while running Cisco IOS Release 12.3(23)BC1.</p> <p>Workaround: There are no known workarounds.</p>
CSCsl92187	<p>Symptom: Change in syntax of cable modem remote-query command.</p> <p>Condition: This issue is observed when the no form of <b>cable modem remote-query</b> command changes the syntax.</p> <p>Workaround: There are no known workarounds.</p>
CSCsq35790	<p>Symptom: Voice over IP (VoIP) packets of Session Initiation Protocol (SIP) are not recognized. The VoIP packets are assigned to normal Committed Information Rate (CIR) queue instead of Low Latency Queuing (LLQ).</p> <p>Condition: This issue is observed when max ds latency information is not included in Dynamic Service Change (DSC) message.</p> <p>Workaround: Configure max ds latency information on cable modem.</p>
CSCso63567	<p>Symptom: Voice call tone dropout of 4500~5000ms observed during bulk call for cable modem.</p> <p>Condition: Not known.</p> <p>Workaround: There are no known workarounds.</p>
CSCsm11169	<p>Symptom: High CPU utilization is observed on a uBR10012 router with the Cisco MC5X20U cable interface line card during cable modem bringup.</p> <p>Condition: This issue is observed when the line card reloads and when there are many cable modems queuing for registration.</p> <p>Workaround: There are no known workarounds.</p>

**Table 35**      *Open Caveats for Cisco IOS Release 12.3(23)BC3 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCso81928	<p>Symptom: Modems in penalty state due to STM configuration are not accessible after linecard switchover.</p> <p>Condition: Not Known, this issue is seen in both the legacy and wideband cable modems.</p> <p>Workaround: Reset the modem.</p>
CSCsr46842	<p>Symptom: The wideband cable modems wrongly appear in the load balance exclude list besides appearing correctly in the load balance pending list.</p> <p>Workaround: There is no workaround.</p>
CSCso57024	<p>Symptom: The Cisco vendor-specific "Wideband Channel ID" option (vendor-specific option 14) does not work.</p> <p>Condition: This issue is observed when using a recent version of Scientific Atlanta wideband DPC2505 modem with the Cisco uBR10012 router.</p> <p>Workaround: There are no known workarounds.</p>
CSCsq01701	<p>Symptom: Resetting the wideband CMs make them come w-online and the upstream STM enforce- rule configuration does not shape their traffic as expected.</p> <p>Condition: This issue can be seen if modems are in penalty state and for some reason get reset at that time.</p> <p>Workaround: Normally modems in penalty state do not get reset. If they get reset, they will come online and not shape the traffic only for that penalty.</p>

## Resolved Caveats for Release 12.3(23)BC3

[Table 36](#) lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(23)BC3.

**Table 36 Resolved Caveats for Cisco IOS Release 12.3(23)BC3**

DDTS ID Number	Description
CSCsm51986	<p>Symptom: CMTS_UNFRAG_CONCAT_BURST_SIZE does not reflect the platform linecard cap.</p> <p>Condition: This occurs when operators are increasing the upstream throughput rate and the CMTS cable-default-phy burst is set to 0. When the maximum concat burst TLV is omitted, a maximum concat burst size of 3044 is assumed by the cable modem. In this case, CMTS admission control is incorrectly using a fixed defined constant of 2000 as maximum burst size, and the flow is rejected.</p> <p>Workaround: For MC28U/MC28UC/MC16U/MC16UXMC520T cards, the maximum burst size should be 4000 and not 2000.</p>
CSCsr05759	<p>Symptom: If the cable modem is rebooted, the CMTS forwards its DHCP Discover via a different VRF than expected. The subsequent DHCP Request is sent via the correct VRF so that it cannot be correlated to the DHCP Offer.</p> <p>Condition: This issue occurs when multiple bundle interfaces having unique VRFs are associated with the same downstream.</p> <p>Workaround: Either terminate VRFs on a single DHCP server ignoring VRF values, or keep clearing the CMs with a script.</p>
CSCsq72700	<p>Symptom: If DSA or DSC-Req is sent by the Embedded Media Terminal Adapter (eMTA) with DOCSIS Nominal Grant Interval set to 0, then cable linecard would crash.</p> <p>Condition: This issue occurs when eMTA with DOCSIS Nominal Grant Interval for a UGS-AD service flow is set to 0.</p> <p>Workaround: Turn off silence suppression.</p>
CSCsm77199	<p>Symptom: If the HTTP secure server capability is present, the switch shows the following error message:</p> <p>%DATACORRUPTION-1-DATAINCONSISTENCY:</p> <p>Condition: This issue occurs if the HTTP server is configured using the <b>ip http server</b> command.</p> <p>Workaround: Disable the HTTP server using the <b>no ip http server</b> command.</p> <p> <b>Note</b> The switch functionality is not affected by this error message.</p>
CSCsq65000	<p>Symptom: The DS load balancing shows an incorrect state for the modular DS channels with HCCP switchovers and revertbacks.</p> <p>Workaround: Clear the load balancing state using the <b>clear cable load-balance state</b> command.</p>
CSCso71588	<p>Symptom: The downstream channel ID is not unique within a Channel Grouping Domain (CGD).</p> <p>Condition: This issue occurs when you configure RF channels with the same downstream channel ID.</p> <p>Workaround: Ensure that all RF channels in a CGD have different downstream channel IDs.</p>

**Table 36** *Resolved Caveats for Cisco IOS Release 12.3(23)BC3 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsq80577	<p>Symptom: After a line card switchover, the downstream channel ID is not changed as expected.</p> <p>Condition: This issue is observed when a line card switchover happens between the working line card and the protecting line card.</p> <p>Workaround: There are no known workarounds.</p>
CSCsq05652	<p>Symptom: Incorrect display of active calls when nRTPS or RTPS is configured.</p> <p>Condition: The RTPS or nRTPS is interpreted as a call in the output of the <b>show cable calls</b> and <b>show cable modem calls</b> commands.</p> <p>Workaround: Use <b>show packetcable gate summary</b> command to check the status of active calls.</p>
CSCsr03421	<p>Symptom: The standby PRE crashes when a linecard has more than 512 ongoing calls.</p> <p>Condition: This issue occurs if two gates with the same offset are on the free gate list.</p> <p>Workaround: Remove the standby PRE.</p>
CSCsq66130	<p>Symptom: Flowbits keep asserting after an OIR is performed on a SPA, and a traceback is also observed when the <b>show pxf cpu queue</b> command is used.</p> <p>Condition: This problem is observed with the SPA OIR in Cisco IOS Release 12.3(23)BC.</p> <p>Workaround: There are no known workarounds.</p>
CSCsr23126	<p>Symptom: Upstream load balancing breaks with DOCSIS 3.0 certified modems in a w-online(pt) state.</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running Cisco IOS Release 12.3(23)BC.</p> <p>Workaround: There are no known workarounds.</p>
CSCsj12495	<p>Symptom: In a high availability configuration with multiple PREs, the standby PRE might reload when a new line card is inserted.</p> <p>Condition: This issue occurs when inserting a new line card in the chassis.</p> <p>Workaround: There are no known workarounds.</p>
CSCsq05424	<p>Symptom: A wideband CM that fails the BPI+ negotiation shows w-online on the CMTS instead of w-reject(pk) or w-reject(pt).</p> <p>Condition: This issue occurs when the CMTS deems that the BPI+ authorization request sent by the wideband CM is invalid. This will result in the CM staying in the w-online state instead of moving to the w-reject (pk) state. Thus, the CM appears operational even though it is unable to communicate data traffic with the CMTS.</p>
CSCsq47785	<p>Symptom: The secondary PRE serial number of the Cisco uBR10012 router is shown as "N/A".</p> <p>Workaround: Use <b>show diag</b> command to display the serial number.</p>

**Table 36 Resolved Caveats for Cisco IOS Release 12.3(23)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsq53782	Symptom: A false INFO level alarm is raised when using non-default configuration for "max-ports" and "connector" on upstream port, even when the port is actually up and running. Workaround: There are no known workarounds.
CSCsq79058	Symptom: Unable to set the MIB objects "ccwbRFChanQamIPAddress", "ccwbRFChanQamMacAddress" and "ccwbRFChanQamUdpPort" separately. Workaround: Set the MIB objects "ccwbRFChanQamIPAddress", "ccwbRFChanQamMacAddress" and "ccwbRFChanQamUdpPort" in single instruction set.
CSCsr57508	Symptom: Interfaces of C6/1 are dropping to offline status resulting in modems failure to register with CLC. Condition: The cable interface is using more logical upstream channels than the number of physical channels when frequency stacking is enabled (shared connector). Workaround: There are no known workarounds.
CSCso78689	When an interface, usually a line card (Gigabit Ethernet), with an output service policy with random detect is removed, an assertion failure results. These assertion messages are logged every 10 seconds. Condition: This issue is observed if an interface with an output service policy with random detect is removed (commonly the result of removing a line card). Workaround: Remove the output service policy from the interface prior to removal of the line card.
CSCsl87023	Symptom: The <b>Running-configuration</b> and <b>show controllers</b> commands show different values for upstream center frequency.
CSCsq83033	Symptom: All the WB and NB modems go offline after a combination of steps of linecard switchover / revertback and interface <b>shutdown / no_shutdown</b> . Workaround: There are no known workarounds.
CSCso58293	Symptom: One CM on 8/0/1 bay dropped offline and disappeared from show cable modem command. Condition: The issue is observed when the switch over is performed after a Guardian host switch over (slot 7/0). Workaround: Make sure that each mac domain has the same number of MC interface during configuration.
CSCso73405	Symptom: Traceback was observed on both RPs. Condition: LCSO during PRE bulk sync. Workaround: There are no known workarounds.
CSCso74192	Symptom: The show cable clock command returned incorrect value for number of TCC cards. Condition: Insert new DTCC cards into slot 1/1 and 2/1 and do a PRE2 switchover. Workaround: Perform another PRE2 switchover.

Table 36 Resolved Caveats for Cisco IOS Release 12.3(23)BC3 (continued)

DDTS ID Number	Description
CSCso76704	<p>Symptom: While performing PRE2 switchover, the following errors were displayed:</p> <pre>F241-38-03-UBR10K-1#redundancy force-failover main-cpu Proceed with switchover to standby PRE? [confirm]y % HCCP 1 50 Switchover in progress. HA system in transient state, switchover aborted.</pre> <p>One of the reason is that one of the cable linecard is locked out. It should indicate it is a lockout instead of switchover.</p> <p>Condition: When one or more cable linecard is locked out, the PRE2 switchover gives misleading message.</p> <p>Workaround: Run <b>show hccp detail   include lockout</b> command before PRE2 switchover.</p>
CSCso76808	<p>Symptom: Primary downstream service flow with non-zero DOCSIS priority appears to get synced to the standby PRE with priority set to zero. This results in the corresponding queues being created on the standby PRE prior to switchover with incorrect parameters.</p> <p>Condition: Set DS priority in CM config file.</p> <p>Workaround: There are no known workarounds.</p>
CSCso79703	<p>Symptom: Wideband cable modems related to interface drops offline.</p> <p>Condition: This issue is observed when:</p> <ol style="list-style-type: none"> <li>a. HCCP switchover is performed between working interface and protecting interface</li> <li>b. Run <b>modify guardian host</b> command and wait for WCM to come back w-online, and</li> <li>c. HCCP switchover is performed back to working interface</li> </ol> <p>Workaround: There are no known workarounds.</p>
CSCso82323	<p>Symptom: The primary PRE crashes after PRE switchover.</p> <p>Condition: This issue is observed when the following steps are performed with LC5/1 linecard protected and working LC7/0:</p> <ol style="list-style-type: none"> <li>1. Switchover from 7/0 to 5/1.</li> <li>2. Shutdown one of active protect interface, such as 5/1/2.</li> <li>3. Revert back to 7/0 using <b>redundancy linecard revertback 7/0</b> command.</li> <li>4. PRE switchover using <b>reduncancy force-failover main-cpu</b> command.</li> <li>5. Perform the <b>noshutdown 5/1/2</b> command, causes crash in new active PRE.</li> </ol> <p>Workaround: Do not shutdown protected linecard interface.</p>

**Table 36 Resolved Caveats for Cisco IOS Release 12.3(23)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCso86994	<p>Symptom: The standby PRE crashes.</p> <p>Condition: This issue is observed when the following steps are performed with LC5/1 line card protected and working LC7/0:</p> <ol style="list-style-type: none"> <li>1. Switchover from 7/0 to 5/1.</li> <li>2. Shutdown one of active protected interface, such as 5/1/2.</li> <li>3. Boot up standby PRE</li> <li>4. Run the <b>noshutdown 5/1/2</b> command</li> <li>5. Revert back to 7/0 using <b>redundancy linecard revertback 7/0</b> command. This command causes crash in standby PRE.</li> </ol> <p>Workaround: Do not shutdown protected LC interface.</p>
CSCso99609	<p>Symptom: The protect linecard does not clear the SPA entry in the output of show hw-module bay all association wideband command after the linecard revertback.</p> <p>Condition: This problem is observed in two conditions:</p> <ol style="list-style-type: none"> <li>1. Linecard switchover and revertback.</li> <li>2. configure and unconfigure CGD from the working linecard.</li> </ol> <p>Workaround: There are no known workarounds.</p>
CSCsq00101	<p>Symptom: Wideband cable modems switch between offline and online states.</p> <p>Condition: This problem is observed in two conditions:</p> <ol style="list-style-type: none"> <li>1. N+1 switchover from W1 (guardian) to Protect.</li> <li>2. Change guardian host to be W2.</li> <li>3. Revert from Protect to W1 (non-guardian).</li> </ol> <p>Workaround: Reset the linecard.</p>
CSCsq02262	<p>Symptom: Based on the HCCP design, IPC timeout should trigger the linecard switchover. However, The IPC timeout does not trigger the linecard switchover but only shuts down the specific interface.</p>
CSCsq08651	<p>Symptom: The banner in the configuration disappears.</p> <p>Condition: This issue occurs after a PRE switchover due to a crash.</p> <p>Workaround: Reapply the configuration.</p>
CSCsq19079	<p>Symptom: Inconsistency in the running configuration details is observed in the PRE modules after the PRE switchover occurs.</p> <p>Condition: The change is observed under the following conditions:</p> <ol style="list-style-type: none"> <li>1. Working linecard failover to Protect linecard.</li> <li>2. Shutdown the w linecard.</li> <li>3. PRE switchover.</li> </ol> <p>Workaround: There are no known workarounds.</p>

**Table 36** *Resolved Caveats for Cisco IOS Release 12.3(23)BC3 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsq23851	<p>Symptom: Establishing communication or pinging the wideband cable modem was unsuccessful after the linecard switchover occurred.</p> <p>Condition: This problem is observed when the <b>shutdown / no shutdown</b> commands were run on the primary channel and the wideband cable modem was in the online(pt) state.</p> <p>Workaround: Do not enable the Baseline Privacy Interface (BPI).</p>
CSCsq24138	<p>Symptom: The sh hw-module bay 1/0/0 association wideband-channel commands shows incorrect NB channel entries for the wideband interface under active protect LC.</p> <p>Condition: Both guardian and mac domain host are on the same linecard, and shutdown/no shutdown command is run on the active protect interface.</p> <p>Workaround: Do not shutdown the protect interface.</p>
CSCsq50907	<p>Symptom: When an HCCP switchover is done, one of the upstream channels on each frequency stacked ports lose communication to the modems connected to it.</p> <p>Condition: The show controller command output does not show the upstream port assignments for the affected upstream channels.</p> <p>This issue is observed on a Cisco uBR10012 router running Cisco IOS 12.3(23)BC2 release.</p> <p>Workaround: There are no known workarounds.</p>
CSCsq77834	<p>Symptom: The wideband cable modem does not come online as w-online when the working linecard is reset. This condition is followed by resetting the protect linecard after the working linecard comes online.</p> <p>Workaround: There are no known workarounds.</p>
CSCsq79201	<p>Symptom: In a narrowband over SPA setup, some modems get stuck in the init(d) state after multiple switchover switch back occurs.</p> <p>Condition: This issue is observed on a Cisco uBR10012 router running Cisco IOS 12.3(23)BC2 release.</p> <p>Workaround: Clear the ARP table entry for the affected modem.</p>
CSCsq84686	<p>Symptom: All modems on a given upstream may go offline.</p> <p>Workaround: Run the <b>shutdown/no shutdown</b> commands on the cable upstream interface:</p> <ol style="list-style-type: none"> <li>1. cable upstream shutdown</li> <li>2. no cable upstream shutdown</li> </ol>
CSCsq49714	<p>Symptom: A problem occurs when the cable modem is locked on a modular-cable interface downstream with no available upstreams on the fiber node.</p> <p>Workaround: There are no known workarounds.</p>

**Table 36** Resolved Caveats for Cisco IOS Release 12.3(23)BC3 (continued)

DDTS ID Number	Description
CSCsj40978	<p>Symptom: The Cisco uBR10012 router fails to boot or fails when a request for BPI+ session is received.</p> <p>Condition: This issue is observed when the US and EU root certificates are not present on the file system.</p> <p>Workaround: Ensure that the US and EU certificates are present in the file system before security is enabled.</p>
CSCsr63088	<p>Symptom: Static upstream load balance was unbalanced in some cases.</p> <p>Conditions: This issue is observed when static load balance was configured on an interface with more than one upstreams.</p> <p>Workaround: Enable dynamic load balancing.</p> <p> <b>Note</b> If interface has more than two upstreams configured, this issue might be observed.</p>

## Open Caveats for Release 12.3(23)BC2

Table 37 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(23)BC2.

**Table 37** Open Caveats for Cisco IOS Release 12.3(23)BC2

DDTS ID Number	Description
CSCek41611	<p>Cisco uBR10-MC5X20U line cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>
CSCsk50223	<p>In a Cisco uBR10012 router with the Cisco MC5X20U-D cable interface line card, downstream cable modems are not synching with the CMTS.</p> <p>The issue is found on routers running Cisco IOS Release 12.3(13a)BC6.</p> <p>Workaround: Run the <b>cable power off</b> command on the Cisco MC5X20U-D line card.</p>
CSCs150048	<p>Modems cannot register on modular-cable downstreams when they use config files that have downstream llq (max downstream latency) set, but do not have minimum and maximum DS rate configured.</p> <p>These modems are stuck in reject(c) state</p> <p>Workaround: Add minimum and maximum DS rate in the downstream service flow encoding in the configuration file.</p>

**Table 37** Open Caveats for Cisco IOS Release 12.3(23)BC2 (continued)

DDTS ID Number	Description
CSCso30731	<p>A Cisco uBR10012 router with ESR-PRE2 will crash because a chunk element is corrupted.</p> <p>The crash occurs on routers with ESR-PRE2 running Cisco IOS Release 12.3(21a)BC3.</p> <p>There are no known workarounds.</p>
CSCs157014	<p>An unexpected crash occurs when executing the <b>show ip interface brief</b> command soon after load and bootup.</p> <p>There are no known workarounds.</p>
CSCs172140	<p>Few modems, with similar configurations, were stuck in the <b>init(io)</b> state and could not proceed further.</p> <p>Workaround: Execute <b>clear cable modem [mac-address] delete</b> command.</p>
CSCs173237	<p>On a uBR10012 router with 24 RF channel SPA, when the <b>show controller cable x/x/x downstream</b> and <b>show interface modular-cable 1/0/x:x downstream</b> commands are run, downstream flow counters show incorrect values. This is noticed when wideband modems are in wb-online state.</p> <p>There are no known workarounds.</p>
CSCsm11169	<p>High CPU utilization is observed on a uBR10012 router with the Cisco MC5X20U cable interface line card during cable modem bringup.</p> <p>The high value is observed when the line card reloads and when there are many cable modems up for registration.</p> <p>There are no known workarounds.</p>
CSCsm12010	<p>In a uBR10012 router, packets sent from the cable modems to some Customer Premise Equipments (CPE) are lost due to possible hardware ARP information.</p> <p>This is observed when 2000 or more wideband modems are connected to a uBR10012 router.</p> <p>Workaround: Run <b>clear ip arp &lt;mac-address&gt;</b> command to get a new IP address.</p>
CSCsm47906	<p>Cable modems drop offline when pre-equalization is enabled. This is also observed when a severe noise is found on the hybrid fiber-coaxial (HFC) system.</p> <p>Workaround: Disable and re-enable pre-equalization. In other words, execute:</p> <p><b>no cable upstream 0 equalization-coefficient</b>  <b>cable upstream 0 equalization-coefficient</b></p>
CSCsm54577	<p>The following Fan Tray missing error occurs.</p> <pre>Oct 17 22:12:47.869: %UBR10K_ALARM-6-INFO: ASSERT CRITICAL fan-tray-slot Fan tray missing Oct 17 22:12:47.869: %CI-1-NOFAN: Fan tray empty Oct 18 05:47:23.287: %UBR10K_ALARM-6-INFO: CLEAR CRITICAL fan-tray-slot Fan tray missing Oct 18 05:47:23.287: %CI-6-BLOWEROK: Fan tray module OK</pre> <p>Workaround: Replacement of the Fan module does work in a few instances.</p>

**Table 37** *Open Caveats for Cisco IOS Release 12.3(23)BC2 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCso31732	<p>Cable modems may fail to come online on a Cisco uBR-MC5X20S cable interface line card in a UBR10012 router due to a bad offset message:</p> <pre>UBR10000-4-BADTXOFFSET: Bad timing offset &lt;negative value&gt; detected for cable modem &lt;mac&gt;</pre> <p>This issue is seen only on MC5x20S cards when the rate-adapt feature has been enabled.</p> <p>Workaround: Disable the rate-adapt feature for the MC5x20S upstreams.</p>
CSCso07595	<p>High CPU utilization is observed on a uBR10012 router with the Cisco MC5X20U-D cable interface line card after a PRE2 switchover.</p> <p>This is observed on a Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC6 with PRE2 and MC5X20U-D line cards.</p> <p>Workaround: Run the <b>cable power off</b> command on the line card.</p>
CSCso49733	<p>In a cluster of Cisco uBR10012 routers supporting the wideband service, the following errors may be observed.</p> <ul style="list-style-type: none"> <li>• Most wideband cable modems are stuck in the init(io) state</li> <li>• Pinging fails between the cable modems</li> <li>• <b>show hw-module bay all counters rf-channel</b> command displays ts count as 0 in the 3,5,7 RF channels</li> <li>• Special log message is not displayed before the error</li> </ul> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Reload the system</li> <li>2. Switchover PRE twice and remove and re-configure all wideband configurations (modular cable, wideband interface and fiber node)</li> </ol>
CSCso16183	<p>SNMP may report different speeds and modulation types for upstream channels that were configured for the same type of modulation. Output of <b>show controller</b> command still shows the configured value.</p> <p>This was seen on a Cisco uBR10012 router running Cisco IOS Release 12.3(17b)BC4 with cable line card interfaces configured for 16 QAM.</p> <p>There are no known workarounds.</p>
CSCso57024	<p>When using a recent version of Scientific Atlanta wideband DPC 2505 modem with the Cisco uBR10012 router, the Cisco vendor-specific "Wideband Channel ID" option (vendor-specific option 14) has no effect.</p> <p>There are no known workarounds.</p>
CSCso61562	<p>When both the TCC+ cards are down, the Cisco uBR10012 router displays a message that a working TCC card is not available.</p> <p>After PRE2 switchover, the TCC+ down state is not reported. This issue persists even after reverting the PRE2 switchover.</p> <p>Workaround: Periodically check the TCC+ card.</p>

**Table 37** Open Caveats for Cisco IOS Release 12.3(23)BC2 (continued)

DDTS ID Number	Description
CSCso61937	The Cisco uBR10-MC5X20U line card crashes due to memory corruption. This issue is observed while running Cisco IOS Release 12.3(23)BC1. There are no known workarounds.
CSCso63578	Memory leak in Pool Manager occurs with a uBR10012 router running Cisco IOS 12.3(23)BC1. A combination of best effort data traffic, UGS voice traffic and SNMP polling results in the memory leak. There are no known workarounds.
CSCso72002	A PRE2 crash results in an HCCP failover with the following system log. %HCCP-5-FAILURE: Grp 1 Mbr 71 Working: received failure notice-link down (suspend timer). %HCCP-5-STANDBY: Grp 1 Mbr 71 Working: change state from active to standby cause: link down (suspend timer). This occurs on a uBR10012 router running 12.3(23)BC1 with 1700 or more cable modems, 280+ MTAs, upstream utilization approximately 50-80%, and downstream utilization approximately 54-71%. There are no known workarounds.
CSCso74192	The <b>show cable clock</b> command wrongly displays number of TCC cards in the chassis. This occurs when new DTCC cards are inserted into slot 1/1 and 2/1 followed by a PRE2 switchover. Workaround: Perform another PRE2 switchover.
CSCso76579	HCCP failover may occur even when connectivity with the RF switch has failed. This occurs when a uBR10012 router running Cisco IOS Release 12.3(23)BC1 is configured for 8+1 global HCCP. There are no known workarounds.
CSCso76617	A Cisco uBR10-MC5X20U cable line card crashes due to corrupted redzone block, and reports a Check Heaps CPU Hog message. This is observed on a uBR10012 router running Cisco IOS Release 12.3(23)BC1 with regular data traffic and intermittent voice traffic. There are no known workarounds.
CSCso78689	When an interface, usually a line card (Gigabit Ethernet), with an output service policy with random detect is removed, an assertion failure results. These assertion messages are logged every 10 seconds. Workaround: Before removing the line card, remove the output service policy from the interface.
CSCso82923	The <b>cable dcu-upstream-disable &lt;mac-address&gt; [enable disable]</b> command has no effect, and the configuration is not retained. Workaround: Provision the cable modem with a DOCSIS 1.1 QOS profile of 10 Kbit/sec upstream + 10 kbit/sec downstream, BPI+ enabled, and PC access denied. Use a max-cpe of 1.

**Table 37**      **Open Caveats for Cisco IOS Release 12.3(23)BC2 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCso83622	<p>The PEM power consumption data is not displayed when the <b>show controllers clock-reference</b> command is run on a uBR10012 router when DTI clock cards are used.</p> <p>There are no known workarounds.</p>
CSCso92184	<p>Many wideband cable modems go down. This occurs when the line cards are not configured with the <b>modular-host subslot</b> command.</p> <p>Workaround: Install 2 SPA cards and 2 MC520U-D cards for wideband cable modems.</p>
CSCso96838	<p>Secondary PRE2 crashes when the following exceptions are run.</p> <ul style="list-style-type: none"> <li>• no exception-slave core-file ubr3</li> <li>• no exception-slave dump 172.18.98.28</li> <li>• no exception core-file ubr3</li> <li>• no exception dump 172.18.98.28</li> </ul> <p>Workaround: Do not remove the exception.</p>
CSCso98714	<p>Scientific Atlanta DPC2100r1 cable modems take a long time to come online.</p> <p>This occurs only with the Scientific Atlanta DPC2100r1 modems after upgrading the uBR10012 router from Cisco IOS Release 12.3(17b)BC4 to 12.3(23)BC or 12.3(23)BC1.</p> <p>Workaround: If the cable modem comes online, reset the modem from the CMTS (via the CLI) or while in init(r1) manually set the downstream frequency on the modem's web page to make it come online immediately. If the cable modem is using upstream load balancing, remove it.</p>
CSCsq00921	<p>The upstream transmit power level on the cable modem gets a higher value with the Cisco uBR10-MC5X20H line card compared to the upstream line card.</p> <p>This occurs when the cable modem is connected to the Cisco uBR10-MC5X20H line card.</p> <p>Workaround: Lower the value using the <b>cable upstream &lt;port#&gt; power-level &lt;value&gt;</b> command.</p>
CSCsq01701	<p>When wideband cable modems are on penalty, resetting these modems will make them come w-online and the upstream STM enforce rule will not shape their traffic as expected.</p> <p>This issue can be seen if modems are on penalty and for some reason get reset at that time.</p> <p>Workaround: Normally modems on penalty do not get reset. If they get reset, they will come online and not shape the traffic only for that penalty.</p>
CSCsq05424	<p>Wideband cable modems that fail BPI+ negotiation show w-online on the CMTS instead of w-reject(pk) or w-reject(pt).</p> <p>There are no known workarounds.</p>
CSCsq05652	<p>Incorrect display of active calls when nRTPS is configured.</p> <p>There are no known workarounds.</p>

**Table 37**      *Open Caveats for Cisco IOS Release 12.3(23)BC2 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsq08644	PXF crashes. This occurs on a uBR10012 router running 12.3(23)BC1 with the DS and US congested/saturated with regular traffic, including commercial traffic and voice traffic, and US utilization of 97%.  There are no known workarounds.
CSCsq08651	The banner in the configuration disappears. This occurs after a PRE switchover due to a crash.  Workaround: Reapply the configuration.
CSCsq12235	Wideband modems do not come w-online following Modular Cable Controller configuration change.  There are no known workarounds.

## Resolved Caveats for Release 12.3(23)BC2

[Table 38](#) lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(23)BC2.

**Table 38 Resolved Caveats for Cisco IOS Release 12.3(23)BC2**

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCso81854	<p>Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.</p> <p>To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.</p> <p>Cisco has released free software updates that address these vulnerabilities.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080708-dns">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080708-dns</a></p> <p>This security advisory is being published simultaneously with announcements from other affected organizations.</p>
CSCsm50944	<p>A high CPU value is observed when many host IP addresses of modems are registered with static IP addresses. This is observed when some subinterfaces are configured using <b>cable source-verify</b> command and other subinterfaces in the same bundle are configured using <b>cable source-verify dhcp</b> command.</p> <p>Workaround: Use <b>cable source-verify dhcp</b> command on both the subinterfaces. As for the static IP addresses, reserve these addresses in the DHCP server.</p>
CSCsg35077	<p>A device that is running Cisco IOS software may crash during processing of an Internet Key Exchange (IKE) message.</p> <p>Workaround: Customers that do not require IPsec functionality on their devices can use the <b>no crypto isakmp enable</b> command in global configuration mode to disable the processing of IKE messages and eliminate device exposure.</p> <p>If IPsec is configured, this bug may be mitigated by applying access control lists that limit the hosts or IP networks that are allowed to establish IPsec sessions with affected devices. This assumes that IPsec peers are known. This workaround may not be feasible for remote access VPN gateways where the source IP addresses of VPN clients are not known in advance. ISAKMP uses port UDP/500 and can also use UDP/848 (the GDOI port) when GDOI is in use.</p>

**Table 38** *Resolved Caveats for Cisco IOS Release 12.3(23)BC2 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCsi95211	<p>The Tunnel maximum transmission unit (MTU) value is reset to 1514 bytes.</p> <p>This occurs when the ip mtu value that is configured on a tunnel interface is greater than 1514 bytes and an IP address is subsequently assigned to the Tunnel interface.</p> <p>Workaround: Re-configuring the ip mtu value after the IP address has been configured restores the ip mtu value.</p>
CSCsg54174	<p>On a Cisco uBR10012 router, with traffic passing through the Gigabit Ethernet interface, a bit rate of zero is displayed when running the <b>show interface</b> command.</p> <p>This is observed when a high volume of traffic (at least 600 mbps) is being transmitted through a Gigabit Ethernet interface and there are large number of interfaces (atleast 10000) active on the router.</p> <p>There are no known workarounds.</p>
CSCso91691	<p>When multicast and P2P queues are configured on the same interface, the exceed action for the multicast flow is set to Tx.</p> <p>There are no known workarounds.</p>
CSCsi03598	<p>PRE 2 unexpectedly reloads and goes into a loop.</p> <p>This issue occurs when removing the existing flash card from slot1 of PRE2 and inserting another card and running a <b>dir all</b> command.</p> <p>Workaround: Remove the flash card.</p>
CSCsk12224	<p>After LC switchover, modems cannot be assigned with any CM-created DOCSIS 1.0 QoS profile. The <b>cable modem qos profile</b> command works but the profile does not get assigned</p> <p>The defect is seen in all software releases.</p> <p>Workaround: Delete the modem before assigning the CM-created QoS profile using the <b>clear cable modem delete</b> command.</p>
CSCsq02290	<p>Line card crashes when configuring <b>no weekend</b> after configuring <b>weekend off</b> on a uBR10012 router.</p> <p>Workaround: The crash can be avoided by always un-configuring the complete enforce-rule when changes are required and then configure again as a new enforce-rule.</p>

**Table 38 Resolved Caveats for Cisco IOS Release 12.3(23)BC2 (continued)**

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCsk85933	<p>A uBR10012 router running 12.3(17b)BC3 may report Cable Modems stuck in <b>init(rc)</b> state on certain Upstream Interfaces. Very high number of Input queue drops are also observed under the corresponding Downstream interfaces.</p> <p>This problem has only been observed on uBR10012 router with MC5x20H-D card.</p> <p>Workaround: Reseating the line card will bring all the Cable Modems back to online.</p>
CSCsl42554	<p>All CMs became offline with no alert or log message. When <b>clear cable modem all delete</b> command was executed, no CM was ranging. When checked, upconverter signal was ok and ucd counter also normal.</p> <p>This issue is observed in routers with the Cisco MC520H linecard.</p> <p>Workaround: Use <b>cable downstream rf-shutdown</b> and <b>no cable downstream rf-shutdown</b> commands.</p>
CSCsl55949	<p>A Parallel Express Forwarding (PXF) processor crash causes the PRE2 to crash as well. The PRE2 crash follows due to the memory allocation error:</p> <pre>%SYS-3-OVERRUN: Block overrun at 1A91D098 (red zone 45BED810)</pre> <p>This occurrence is found in Cisco IOS Release 12.3(17b)BC9 with the PXF enabled on the ESR-PRE2.</p> <p>Workaround: Disable the PXF processor.</p>
CSCsl73926	<p>On a wideband SPA (Shared Port Adapter), when one SFP module is disconnected the other module does not connect as expected.</p> <p>There are no known workarounds.</p>
CSCsl74859	<p>If the <b>show cable modem</b> command is used after a PRE switchover, cable modems are duplicated with the same MAC address.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(00)BC3.</p> <p>There are no known workarounds.</p>
CSCsl98243	<p>Syslog messages are logged on the syslog server using one of the Gigabit Ethernet interfaces instead of the specified loopback interface.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(21a) BC3.</p> <p>Workaround: Reapply the <b>no logging source-interface Loopback0</b> and <b>logging source-interface Loopback0</b> commands.</p>

**Table 38** Resolved Caveats for Cisco IOS Release 12.3(23)BC2 (continued)

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCsm15646	<p>When the CMTS is configured with more than 32 wideband groups, the wideband interface counters stop updating even with continuous traffic flow.</p> <p>Workaround: It is better to configure less than 32 Wideband interfaces.</p>
CSCsm31562	<p>Cable modems do not return to online state when an operator executes a <b>shut/no-shut</b> command on the protect interface or resets the Protect linecard even after the Protect linecard comes up. This is observed on a uBR10000 router when the Protect linecard is active while the Working linecard is down.</p> <p>Workaround: If the Working linecard is brought back up in the standby mode, then the modems do come online on the Protect linecard.</p>
CSCsm33336	<p>Output of the <b>show controller cable x/x/x</b> command displays previous entries of narrowband (NB) channel when its <i>channel-id</i> is changed. However it does not impact the modem registration.</p> <p>Workaround: Do not change the <i>channel-id</i> value of the NB channel after configuration.</p>
CSCsm46631	<p>Symptom: There are discrepancies in the outputs of <b>show diag</b> and <b>show inventory</b> commands for the Cisco 520U and 520H cable interface linecards. The mismatch occurs in PID, SN and VID values of the output.</p> <p>Condition: The issue is found on routers running Cisco IOS Release 12.3(21a)BC4 and later Cisco IOS releases.</p> <p>Workaround: There is no workaround.</p>
CSCsm52934	<p>The previously disabled JIB upstream port becomes enabled after the Cisco 520 line card is reset.</p> <p>Workaround: Run the <b>shut/no shut cable interface</b> command to correct the anomaly.</p>
CSCsm55512	<p>Tracebacks occur every time when INVALIDSIDPOSITION error is displayed in a CMTS that has a large number of cable modems with a few going offline.</p> <p>There are no known workarounds.</p>
CSCsm55957	<p>The Channel Grouping Domain (CGD) configuration does not work correctly on the Protect linecard after the linecard reverts and the working linecard takes over.</p> <p>Workaround: It is recommended to not make changes to the CGD on the Protect linecard.</p>

**Table 38 Resolved Caveats for Cisco IOS Release 12.3(23)BC2 (continued)**

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCsm56649	<p>The server trace path is not updated correctly.</p> <p>There are no known workarounds.</p>
CSCsm58028	<p>In the uBR10000 series router, alignment tracebacks and corrections in list enqueue and remove functions may be observed on the cable linecard during linecard N+1 switchover.</p> <p>This is usually seen after several Linecard switchovers and reverts along with PRE switchovers.</p> <p>There are no known workarounds.</p>
CSCsm60481	<p>The <b>clear cable wideband reset</b> command resets all modems that are wideband capable and wideband online instead of resetting only the wideband modems.</p> <p>There are no known workarounds.</p>
CSCsm65883	<p>Modems do not go online on P after a linecard failover from W to P when the keepalive failure is already configured. Modems also do not go online on W after a revertback from P to W.</p> <p>This issue is observed only when another linecard failure occurred before the triggered keepalive linecard failover.</p> <p>There are no known workarounds.</p>
CSCsm75724	<p>The following messages are seen during the boot up of the CMTS.</p> <pre>*Feb 18 04:58:39.763: %UBR10KTCC-4-CHG_CLK_REF: Clock reference source set to Invalid for TCCplus card 1/1</pre> <p>In TCC state machine, TCC card reports its best clock reference, which later can be corrected by PRE. For Shiplbells card that starts in a backup role, reported clock reference input is always "Invalid clock". Later, PRE reconfigures this mode for Active card, so functionally the system works properly.</p> <p>Workaround: If reported card role is not active, do not update the input clock value of TCC+ card with the reported clock reference, since this value is always "Invalid".</p>

Table 38 Resolved Caveats for Cisco IOS Release 12.3(23)BC2 (continued)

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCsm79540	<p>The <b>show inventory</b> command displays multiple duplicates of the Power Entry Module (PEM) entries.</p> <p>This is observed on the Cisco uBR10012 router with redundant ESR-PRE2 and PEM.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. PRE Failover</li> <li>2. Full reload</li> </ol> <p>However these tasks only clear the duplicates to the original true value before adding duplicates over time.</p>
CSCsm84974	<p>The configuration of Multicast QoS and ToS-based P2P traffic management results in the multicast traffic to which the QoS is applied, to be limited to 1Mbps.</p> <p>This is observed when both features are enabled.</p> <p>Workaround: Do not run both Multicast QoS and ToS-based P2P on the same interfaces.</p>
CSCsm89100	<p>Error messages such as</p> <pre>"Failed updating link queue for Wideband-Cable 1/0/0:0 on RF channel 0."</pre> <p>is printed on the Standby PRE's console after a new RF channel is added to an existing wideband cable interface.</p> <p>The problem occurs when a wideband cable interface is configured with <b>cable dynamic-bw-sharing</b> command and a new RF channel with valid frequency and IP address is added to this interface. Services provided by the CMTS is unaffected however.</p> <p>There are no known workarounds.</p>
CSCsm89818	<p>The upstream interface information is not displayed correctly while running the <b>show packetcable gate sum</b> command. This is observed after Dynamic Channel Change (DCC) happens.</p> <p>There are no known workarounds.</p>
CSCsm93847	<p>When ATDMA is run for DOCSIS 2.0, the 1.x cable modems will be moved to a port which can not be registered by these modems.</p> <p>Workaround: Run <code>tdma-atdma</code> for all modems in the 3.2 MHz channel width.</p>

**Table 38 Resolved Caveats for Cisco IOS Release 12.3(23)BC2 (continued)**

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCso03676	<p>The LCDOS jacket build is broken after make release failed for obj-c10k-jacket in LCDOS after CSCsl42722 defect.</p> <p>There are no known workarounds.</p>
CSCso04521	<p>The Cisco uBR10012 router may crash when executing the <b>test cable load-balance ucc</b> command.</p> <p>There are no known workarounds.</p>
CSCso08115	<p>The HCCP sync-pulse logic can lead to unexpected resets and/or switchovers of working line cards due to defective Protect line cards.</p> <p>There are no known workarounds.</p>
CSCso27149	<p>DTI interface could be configured even as it is an internal interface.</p> <p>There are no known workarounds.</p>
CSCso30351	<p>After PRE switchover, the cRFStatusLastSwactReasonCode value is wrongly set to activeUnitRemoved(7) when it should be userInitiated(4).</p> <p>There are no known workarounds.</p>
CSCso32342	<p>While removing the rf-bandwidth-percent of the modular interface, the link queue is not removed when the status of the interface is down.</p> <p>This is observed when the <b>no shutdown</b> command is run without bandwidth configuration on the modular interface.</p> <p>There are no known workarounds.</p>
CSCso38313	<p>Symptom: On the Cisco uBR10012 router, the active PRE2 crashes and failover to standby PRE occurs when the Protect linecard is in active state.</p> <p>Condition: This is observed on a router running Cisco IOS Release 12.3(17b)BC4 and configured for global N+1 linecard redundancy (HCCP).</p> <p>Workaround: There is no workaround.</p>
CSCso40318	<p>The RF MIB cRFCfgMaintenanceMode value is inconsistent for the set &amp; get queries. For example, when the cRFCfgMaintenanceMode value is set to true it returns a false.</p> <p>There are no known workarounds.</p>

**Table 38** *Resolved Caveats for Cisco IOS Release 12.3(23)BC2 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCso41832	<p>When the "cable rate-adapt" feature is configured on an upstream of a uBR10000 router, the following issues may be seen.</p> <ul style="list-style-type: none"> <li>• Upstream Wide Failure is observed, and modems are stuck offline on that upstream</li> <li>• Error messages for "Bad Timing Offset" may be seen for some modems with a negative time offset value</li> <li>• Traceback in cmts_serve_ies_in_map</li> </ul> <p>Workaround: Disable the "cable rate-adapt" feature.</p>
CSCso42333	<p>There is no warning message to notify that the fiber node status is invalid after configuring the RF channel into a Channel Grouping Domain (CGD).</p> <p>There are no known workarounds.</p>
CSCso42612	<p>SNMP response is slow when ccwbWBCmStatusValue is polled on the Cisco uBR10012 router.</p> <p>There are no known workarounds.</p>
CSCso42653	<p>During installation of a new chassis with the DTCC card, when modems are moved from the old chassis to the new one, some of the modems do not come online and are stuck in the init(rc) state. Pre-equalization control on the cable modems is also not enabled.</p> <p>Workaround: Change the upstream modulation to the Quadrature Phase-Shift Keying (QPSK) modulation.</p>
CSCso45730	<p>The cable load balancing (LB) group has a cluster of TDMA and ATDMA mode channels. During static load balancing, the 1.x cable modem might be moved to the ATDMA channel based on the load. This problem results in the 1.x cable modem taking a long time to come online.</p> <p>Workaround:</p> <ul style="list-style-type: none"> <li>• Use the UCC or the DCC to move the 2.0 modems to ATDMA only channels.</li> <li>• Avoid configuring the mix capabilities of upstream channels in the same LB group.</li> </ul>
CSCso55748	<p>The CMTS incorrectly generates the GRS when the Gate-Set value is set as zero.</p> <p>This is observed on a uBR10012 router running Cisco IOS Release 12.3(23)BC1 with the PacketCable PCMM feature configured.</p> <p>There are no known workarounds.</p>

**Table 38 Resolved Caveats for Cisco IOS Release 12.3(23)BC2 (continued)**

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCso61633	<p>The uBR10012 router with PRE2 crashes at <code>cmts_hccp_load_config</code>.</p> <p>This is observed on the router running Cisco IOS Release 12.3(23)BC1 and later Cisco IOS releases.</p> <p>There are no known workarounds.</p>
CSCso62075	<p>The total reservable bandwidth value is inconsistent when viewing the outputs of <b>show interface modular-cable x/y/z:w downstream</b>, <b>show interface wideband-cable x/y/z:w</b> and <b>show interface cable x/y/z</b> commands.</p> <p>There are no known workarounds.</p>
CSCso79280	<p>Symptom: A Cisco uBR10012 router with the Cisco UBR10-MC5X20 linecard may fail due to excessive memory allocation failures with low memory errors.</p> <p>Condition: This is observed on the router running Cisco IOS Release 12.3(21a)BC4 with ESR-PRE2 module.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Perform the online insertion and removal (OIR) process on the linecard. OIR instructions can be found at: <a href="http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_linecard_oir_ps2209_TSD_Products_Configuration_Guide_Chapter.html">http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_linecard_oir_ps2209_TSD_Products_Configuration_Guide_Chapter.html</a></li> <li>2. Reset the Hw-module subslot 5/1.</li> </ol>
CSCso84029	<p>Symptom: Upstream traffic is not controlled according to the the penalty enforce class in CMTS routers, when the CM is penalized.</p> <p>Condition: When a CM is a penalized and associated with the penalty service class, US traffic is allowed to exceed the penalty class.</p> <p>Workaround: There is no workaround.</p>
CSCsd11861	<p>Jitter and latency occurs in specific UGS upstream service flows that use LLQ scheduling mode instead of the docsis compliant scheduling mode.</p> <p>This is observed when the upstream LLQ scheduling mode is enabled.</p> <p>There are no known workarounds.</p>

**Table 38** *Resolved Caveats for Cisco IOS Release 12.3(23)BC2 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCsk16894	<p>On a MC520H line card, increasing upstream channel width causes modems to increase transmit power, while decreasing the channel width causes modems to decrease power transmit level.</p> <p>This occurs while the CMTS is reporting the same power received for the modems.</p> <p>Workaround: Change the upstream receive power or change attenuation in combining.</p>
CSCso76323	<p>Parallel Express Forwarding (PXF) bus limits maximum MTU on the uBR10012 routers to 9216 bytes and causes data packets to drop.</p> <p>This issue is observed on the router running Cisco IOS Release 12.3(17)BC onwards.</p> <p>There are no known workarounds.</p>
CSCsq15505	<p>Data could not be sent to the DPC3000 cable modem when the baseline privacy interface (BPI) is enabled in wideband mode.</p> <p>This issue is observed when BPI is enabled and primary downstream is not part of the bonding group.</p> <p>Workaround: Use a primary downstream from within the bonding group.</p>
CSCsq18438	<p>When a modem the DOCSIS 3.0 version comes online on a cable upstream that is configured in mixed mode (tdma-atdma), the modem is brought online in tdma mode though it can support atdma.</p> <p>Workaround: Configure the upstream as an atdma upstream instead of a tdma-atdma upstream.</p>

## Open Caveats for Release 12.3(21a)BC7

Table 39 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC7.

**Table 39**      **Open Caveats for Cisco IOS Release 12.3(21a)BC7**

<b>DDTS ID Number</b>	<b>Description</b>
CSCek41611	<p>Cisco uBR10-MC5X20U cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>
CSCsi03598	<p>PRE 2 unexpectedly reloads and goes into a loop.</p> <p>This issue occurs when removing the existing flash card from slot1 of PRE2 and inserting another card and running a <b>dir all</b> command.</p> <p>Workaround: Remove the flash card.</p>
CSCsi05236	<p>When the Ubr10k Half-Height GE line card is connected to the SCE2000 GE link and both are configured with auto-negotiation, the link does not come up. This problem does not exist for the Full-Height GE.</p> <p>This issue occurs when an Ubr10k Half-Height GE is directly connected to the SCE GE link and auto-negotiation is turned on both links.</p> <p>Workaround: If the auto-negotiation is removed from both GE interfaces, then the link will come up.</p>
CSCso16183	<p>SNMP may report different speeds and modulation types for upstream channels that were configured for the same type of modulation. Output of <b>show controller</b> command still shows the configured value.</p> <p>This was seen on a Cisco uBR10K router running Cisco IOS Release 12.3(17b)BC4 with cable line card interfaces configured for 16 QAM.</p> <p>There are no known workarounds.</p>
CSCso21260	<p>When configuring certain rfsnmp-community string as a redundancy suboption, the CMTS does not automatically create the corresponding <b>snmp-server community</b> &lt;password&gt; view hccp_chansw_snmp_view RW entry resulting in the line card switchover failure.</p> <p>There are no known workarounds.</p>
CSCsk85933	<p>A uBR10012 running 12.3(17b)BC3 may report Cable Modems stuck in init(rc) state on certain Upstream Interfaces. Very high number of Input queue drops are also observed under the corresponding Downstream interfaces.</p> <p>This problem has only been observed on uBR10012 with MC5x20H-D card.</p> <p>Workaround: Reseating the line card will bring all the Cable Modems back to online.</p>
CSCsl06036	<p>Maxcpe functionality is broken with w-online modems. The functionality is working with the same modem in the same image when it registered in the online state.</p> <p>There are no known workarounds.</p>

Table 39 Open Caveats for Cisco IOS Release 12.3(21a)BC7 (continued)

DDTS ID Number	Description
CSCs142554	<p>All CMs became offline with no alert or log message. When <b>clear cable modem all delete</b> command was executed, no CM was ranging. When checked, upconverter signal was ok and ucd counter also normal.</p> <p>This issue is observed in routers with the Cisco MC520H linecard.</p> <p>Workaround: Use <b>cable downstream rf-shutdown</b> and <b>no cable downstream rf-shutdown</b> commands.</p>
CSCs142777	<p>Traceback observed in <code>cmts_cgd_get_active_primary</code> on the secondary PRE when image is upgraded resulting in a SPA FPGA upgrade.</p> <p>Modular cable interfaces are configured with the 12.3(23)BC and associated with a “Channel Grouping Domain” using the <b>downstream modular-cable interface</b> command.</p> <p>There are no known workarounds.</p>
CSCs150048	<p>Modems cannot register on modular-cable downstreams when they use config files that have downstream llq (max downstream latency) set, but do not have min and max DS rate configured.</p> <p>These modems are stuck in reject(c) state</p> <p>Workaround: Add minimum and maximum DS rate in the downstream service flow encoding in the configuration file.</p>
CSCs157014	<p>An unexpected crash occurs when executing a <b>show ip interface brief</b> soon after load and bootup.</p> <p>There are no known workarounds.</p>
CSCs172140	<p>Few modems, with similar configurations, were stuck in the <b>init(io)</b> state and could not proceed further.</p> <p>Workaround: Execute <b>clear cable modem [mac-address] delete</b> command.</p>
CSCs173237	<p>On a uBR10012 router with 24 RF channel SPA, when the <b>show controller cable x/x/x downstream</b> and <b>show interface modular-cable 1/0/x:x downstream</b> commands are run, downstream flow counters show incorrect values. This is noticed when wideband modems are in wb-online state.</p> <p>There are no known workarounds.</p>
CSCsm12010	<p>In a uBR10012 router, packets sent from the cable modems to some Customer Premise Equipments (CPE) are lost due to possible hardware ARP information.</p> <p>This is observed when 2000 or more wideband modems are connected to a uBR10012 router.</p> <p>Workaround: Run <b>clear ip arp &lt;mac-address&gt;</b> command to get a new IP address.</p>
CSCsm23260	<p>Timeout occurs when an Inter-Process Communication (IPC) request to the line card is blocked. The following message is displayed.</p> <pre>%REQGRP-3-SYSCALL: System call for command 42 (slot5/0) : Could not send blocked IPC message (Cause: timeout)</pre> <p>This issue is seen only on different cards that handle more than hundreds of modems.</p> <p>Workaround: Reload the card.</p>

**Table 39 Open Caveats for Cisco IOS Release 12.3(21a)BC7 (continued)**

DDTS ID Number	Description
CSCsm41903	<p>Extended ping can not fragment frames in small form-factor (SFP) ports. This problem occurs in both SFP SX ports and SFP copper ports.</p> <p>Workaround: Do not use extended ping in SFP SX ports and SFP copper ports.</p>
CSCsm47906	<p>Cable modems drop offline when pre-equalization is enabled. This is also observed when a severe noise is found on the hybrid fiber-coaxial (HFC) system.</p> <p>Workaround: Disable and re-enable pre-equalization. In other words, execute:  <b>no cable upstream 0 equalization-coefficient</b>  <b>cable upstream 0 equalization-coefficient</b></p>
CSCsm54577	<p>The following Fan Tray missing error occurs.</p> <pre>Oct 17 22:12:47.869: %UBR10K_ALARM-6-INFO: ASSERT CRITICAL fan-tray-slot Fan tray missing Oct 17 22:12:47.869: %CI-1-NOFAN: Fan tray empty Oct 18 05:47:23.287: %UBR10K_ALARM-6-INFO: CLEAR CRITICAL fan-tray-slot Fan tray missing Oct 18 05:47:23.287: %CI-6-BLOWEROK: Fan tray module OK</pre> <p>Workaround: Replacement of the Fan module does work in a few instances.</p>
CSCsm64439	<p>The chassis serial number is not displayed when the <b>show inventory</b> command is run on the router.</p> <p>This observation is found on a uBR10000 (PRE1-RP) router.</p> <p>There are no known workarounds.</p>
CSCsm84974	<p>The configuration of Multicast QoS and ToS-based P2P traffic management results in the multicast traffic to which the QoS is applied, to be limited to 1Mbps.</p> <p>This is observed when both features are enabled.</p> <p>Workaround: Do not run both Multicast QoS and ToS-based P2P on the same interfaces.</p>
CSCsm87471	<p>The Cisco uBR10-MC5X20H line card crashes resulting in a breakpoint exception.</p> <p>The following error message is reported in the crashinfo file:</p> <pre>cr10k_clc_pre_poll: IPC not up. Reloading Line Card..</pre> <p>This is observed on uBR10012 router in Cisco IOS Release 12.3(21a)BCx or 12.3(23)BC.</p> <p>There are no known workarounds.</p>
CSCsm93847	<p>When ATDMA is run for DOCSIS 2.0, the 1.x cable modems will be moved to a port which can not be registered by these modems.</p> <p>Workaround: Run <code>tdma-atdma</code> for all modems in the 3.2 MHz channel width.</p>
CSCso04521	<p>The Cisco uBR10012 router may crash when executing the <b>test cable load-balance ucc</b> command.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(21a)BC7

Table 40 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC7.

**Table 40** Resolved Caveats for Cisco IOS Release 12.3(21a)BC7

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCsm50944	<p>A high CPU value is observed when many host IP addresses of modems are registered with static IP addresses. This is observed when some subinterfaces are configured using <b>cable source-verify</b> command and other subinterfaces in the same bundle are configured using <b>cable source-verify dhcp</b> command.</p> <p>Workaround: Use <b>cable source-verify dhcp</b> command on both the subinterfaces. As for the static IP addresses, reserve these addresses in the DHCP server.</p>
CSCsl82266	<p>Loop occurs between uBR and CNR during <i>leasequery</i>. At the loop condition, you can see several leasequeries per second and after a while, the loop ends automatically.</p> <p>This issue occurs on following conditions:</p> <ul style="list-style-type: none"> <li>• <b>source-verify dhcp</b> is enabled.</li> <li>• CNR failover setup (Redundant CNR).</li> <li>• The target IP of the leasequery loop should be a CPE which is connected to currently offline CM and ARP entry for the CPE aged out.</li> </ul> <p>There are no known workarounds.</p>
CSCsk74962	<p>Router is experiencing spurious memory access while running the <b>show buffer assigned dump</b> command.</p> <p>This issue does not cause any operational problems.</p> <p>There are no known workarounds.</p>
CSCsl73391	<p>CMTS sysUpTime parameter remains unchanged in IPDR document for all records thus making it unreliable for stop records. Similarly, IPDRcreationTime parameters are the same for interim records and are set to the data collection start time for the IPDR document. These may cause certain accounting issues.</p> <p>This issue occurs when Subscriber Account Management Interface Specification (SAMIS) feature is used.</p> <p>Workaround: Poll the DOCS-QOS-MIB object directly.</p>

**Table 40** Resolved Caveats for Cisco IOS Release 12.3(21a)BC7 (continued)

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCsl61201	<p>CMTS generates duplicate IPDR records for same service identifier (SID). This creates accounting issues for usage-based billing of cable modems.</p> <p>This issue occurs on uBR10012 and uBR7200 platforms running Cisco IOS Release 12.3(17b)BC4 when Subscriber Account Management Interface Specification (SAMIS) feature is used.</p>
CSCsg54174	<p>On a Cisco uBR10012 router, with traffic passing through the Gigabit Ethernet interface, a bit rate of zero is displayed when running the <b>show interface</b> command.</p> <p>This is observed when a high volume of traffic (at least 600 mbps) is being transmitted through a Gigabit Ethernet interface and there are large number of interfaces (atleast 10000) active on the router.</p> <p>There are no known workarounds.</p>
CSCsl55949	<p>A Parallel Express Forwarding (PXF) processor crash causes the PRE2 to crash as well. The PRE2 crash follows due to the memory allocation error:</p> <pre>%SYS-3-OVERRUN: Block overrun at 1A91D098 (red zone 45BED810)</pre> <p>This occurrence is found in Cisco IOS Release 12.3(17b)BC9 with the PXF enabled on the ESR-PRE2.</p> <p>Workaround: Disable the PXF processor.</p>
CSCsl72179	<p>Issuing the <b>shut</b> and <b>no shut</b> command stream causes PXF crash resulting in the "TBB Length" error.</p> <p>This is a rare occurrence.</p> <p>There are no known workarounds.</p>
CSCsl73926	<p>On a wideband SPA (Shared Port Adapter), when one SFP module is disconnected the other module does not connect as expected.</p> <p>There are no known workarounds.</p>
CSCsl77607	<p>Upstream cable filter groups for CM and CPE types do not work. ACLs created by the filter group look correct, but does not block qualifying upstream traffic.</p> <p>This issue is also seen in 12.3(21a)BC4. Downstream filter groups work fine for both CM and CPE types.</p> <p>There are no known workarounds.</p>

Table 40 Resolved Caveats for Cisco IOS Release 12.3(21a)BC7 (continued)

DDTS ID Number	Description
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCs191048	<p>The <b>show tech-support</b> and <b>show cable tech-support</b> commands do not provide information about <b>modular-cable x/y/z</b> and <b>jacket x/y</b> in privileged EXEC mode.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(21a) BC3.</p> <p>Workaround: Manually collect the following data:</p> <ul style="list-style-type: none"> <li>• Show controller jacket x/y</li> <li>• Show controller modular-cable x/y/z</li> </ul>
CSCs198243	<p>Syslog messages are logged on the syslog server using one of the Gigabit Ethernet interfaces instead of the specified loopback interface.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(21a) BC3.</p> <p>Workaround: Reapply the <b>no logging source-interface Loopback0</b> and <b>logging source-interface Loopback0</b> commands.</p>
CSCsm79540	<p>The <b>show inventory</b> command displays multiple duplicates of the Power Entry Module (PEM) entries.</p> <p>This is observed on the Cisco uBR10012 router with redundant ESR-PRE2 and PEM.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. PRE Failover</li> <li>2. Full reload</li> </ol> <p>However these tasks only clear the duplicates to the original true value before adding duplicates over time.</p>
CSCso25691	<p>Cable modems are unable to register on specific groupings of upstream interfaces. All upstreams of the cable interfaces that are mapped to connector 0 to 7 belong to the first group. Similarly, connector 8 to 15 form the second group, and the remaining connector 16 to 19 belong to the third group.</p> <p>For cable interface that has "cable default-phy-burst 0" configuration, the problem can be triggered when large requests are fragmented using a large fragment size.</p> <p>Workaround: Remove the <b>cable default-phy-burst 0</b> configuration.</p>

**Table 40** *Resolved Caveats for Cisco IOS Release 12.3(21a)BC7 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsj85065	<p>A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.</p> <p>Cisco has released free software updates that address this vulnerability.</p> <p>Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl</a></p>
CSCsk16894	<p>On a MC520H line card, increasing upstream channel width causes modems to increase transmit power, while decreasing the channel width causes modems to decrease power transmit level.</p> <p>This occurs while the CMTS is reporting the same power received for the modems.</p> <p>Workaround: Change the upstream receive power or change attenuation in combining.</p>
CSCsk03915	<p>The uBR10000 series router is not filtering some cable downstream packets. The issue is observed for IPv4 packets. The packets are sent from CMTS to CM/CPE and the downstream cable filters configured in the PRE2 of the router fails to filter it. However, it does not affect the functionality of the router and the packets from external sources are filtered as expected.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(23)BC1

Table 41 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(23)BC1.

**Table 41** *Open Caveats for Cisco IOS Release 12.3(23)BC1*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsm50944	<p>A high CPU value is observed when many host IP addresses of modems are registered with static IP addresses. This is observed when some subinterfaces are configured using <b>cable source-verify</b> command and other subinterfaces in the same bundle are configured using <b>cable source-verify dhcp</b> command.</p> <p>Workaround: Use <b>cable source-verify dhcp</b> command on both the subinterfaces. As for the static IP addresses, reserve these addresses in the DHCP server.</p>
CSCek41611	<p>Cisco uBR10-MC5X20U cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>

**Table 41** Open Caveats for Cisco IOS Release 12.3(23)BC1 (continued)

DDTS ID Number	Description
CSCsd14355	The Simple Network Management Protocol (SNMP)-created quality of service (QoS) profile is not available after a Performance Routing Engine (PRE) switchover; the command- created QoS profile is available after switchover.  There are no known workarounds.
CSCsi03598	PRE 2 unexpectedly reloads and goes into a loop.  This issue occurs when removing the existing flash card from slot1 of PRE2 and inserting another card and running a <b>dir all</b> command.  Workaround: Remove the flash card.
CSCsm00986	Traceback occurs when the HCCP (Hot Standby Connection-to-Connection Protocol) member is removed through the console and when the <b>sh hccp channel-switch</b> command is run from the VTY session almost simultaneously.  There are no known workarounds.
CSCsk85933	A uBR10k running 12.3(17b)BC3 may report Cable Modems stuck in init(rc) state on certain Upstream Interfaces. Very high number of Input queue drops are also observed under the corresponding Downstream interfaces.  This problem has only been observed on uBR10K with MC5x20H-D card.  Workaround: Reseating the line card will bring all the Cable Modems back to online.
CSCsl06036	Maxcpe functionality is broken with w-online modems. The functionality is working with the same modem in the same image when it registered in the online state.  There are no known workarounds.
CSCsl10231	A downstream service flow with an associated classifier will have the classifier "match count" initialized to zero if there is a PRE switchover or a reload of the pxf.  This issue occurs on a service flow with a classifier and PRE switchover or pxf reload.  There are no known workarounds.
CSCsl24971	CMTS may generate the traceback given below in an extremely rare situation.  %GENERAL-2-CRITEVENT: MRI Unlink Error: Cable5/0/4  There are no known workarounds. This is an occurrence.
CSCsl37665	Since the service flow is not in active state, "cable service flow activity-timeout 1800" will not help. Another timer which is "Admitted QoS timer" should have kicked in and cleaned it. Since that did not happen it is still an issue.  There is no equivalent command to clean out service flows in admitted state.  Customer has a non-packet VOIP service, and currently have the activity-timeout set to 1800 seconds ( implemented about 4 months ago) this value is what is being placed as the Active QoS timeout .  Workaround: Try clearing the Cable Modem using the <b>clear cable modem</b> command. If there are many flows, you could also try to script it.

**Table 41** *Open Caveats for Cisco IOS Release 12.3(23)BC1 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsl42554	<p>All CMs became offline with no alert or log message. When <b>clear cable modem all delete</b> command was executed, no CM was ranging. When checked, upconverter signal was ok and ucd counter also normal.</p> <p>This issue is observed in routers with the Cisco MC520H linecard.</p> <p>Workaround: Use <b>cable downstream rf-shutdown</b> and <b>no cable downstream rf-shutdown</b> commands.</p>
CSCsl42777	<p>Traceback observed in <code>cmts_cgd_get_active_primary</code> on the secondary PRE when image is upgraded resulting in a SPA FPGA upgrade.</p> <p>Modular cable interfaces are configured with the 12.3(23)BC and associated with a "Channel Grouping Domain" using the <b>downstream modular-cable interface</b> command.</p> <p>There are no known workarounds.</p>
CSCsl43172	<p>Traceback observed during cable line card switchover on the line card becoming active.</p> <p>Modular cable interfaces are configured and associated with a "Channel Grouping Domain" using the <b>downstream Modular-Cable</b> interface command</p> <p>There are no known workarounds.</p>
CSCsl50048	<p>Modems cannot register on modular-cable downstreams when they use config files that have downstream llq (max downstream latency) set, but do not have min and max DS rate configured.</p> <p>These modems are stuck in reject(c) state</p> <p>Workaround: Add minimum and maximum DS rate in the downstream service flow encoding in the configuration file.</p>
CSCsl55949	<p>A Parallel Express Forwarding (PXF) processor crash causes the PRE2 to crash as well. The PRE2 crash follows due to the memory allocation error:</p> <pre>%SYS-3-OVERRUN: Block overrun at 1A91D098 (red zone 45BED810)</pre> <p>This occurrence is found in Cisco IOS Release 12.3(17b)BC9 with the PXF enabled on the ESR-PRE2.</p> <p>Workaround: Disable the PXF processor.</p>
CSCsl57014	<p>An unexpected crash occurs when executing the <b>show ip interface brief</b> command soon after load and bootup.</p> <p>There are no known workarounds.</p>
CSCsl72140	<p>Few modems, with similar configurations, were stuck in the <b>init(io)</b> state and could not proceed further.</p> <p>Workaround: Execute <b>clear cable modem [mac-address] delete</b> command.</p>
CSCsl73237	<p>On a uBR10012 router with 24 RF channel SPA, when the <b>show controller cable x/x/x downstream</b> and <b>show interface modular-cable 1/0/x:x downstream</b> commands are run, downstream flow counters show incorrect values. This is noticed when wideband modems are in wb-online state.</p> <p>There are no known workarounds.</p>

**Table 41**      **Open Caveats for Cisco IOS Release 12.3(23)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCs173926	<p>On a wideband SPA (Shared Port Adapter), when one SFP module is disconnected the other module does not connect as expected.</p> <p>There are no known workarounds.</p>
CSCs180669	<p>Jitter in the Best Effort (BE) traffic is observed when there is a LLQ traffic load on an interface.</p> <p>Workaround: Send LLQ traffic stream and BE traffic stream to the cable interface.</p>
CSCs186251	<p>On a uBR10K platform, the following issues are observed while upgrading from ESR-PRE1 to ESR-PRE2, with multiple cable bundled interfaces.</p> <ul style="list-style-type: none"> <li>• High latency to CPE hosts</li> <li>• Low throughput</li> <li>• TCP Timeout and TCP session reset</li> </ul> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Disable the <b>cable source-verify dhcp</b> command</li> <li>2. Clear the temporary arp cache</li> <li>3. Run <b>cable arp</b> command</li> <li>4. Run <b>no cable source-verify [dhcp]</b> command on one of the bundled interfaces</li> </ol>
CSCs192207	<p>Huge punt packets cause the uBR 10012 router PRE-2 memory to exhaust and eventually crash.</p> <p>This occurs while sending traffic with random source or destination IP address and while sending traffic to a few cable modems.</p> <p>There are no known workarounds.</p>
CSCs196432	<p>The association between a customer premises equipment (CPE) and a cable modem (CM) is lost after an N+1 switchover even though the host route determined by the Routing Information Protocol (RIP) appears in the VPN routing/forwarding (VRF) table.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a) BC2.</p> <p>Workaround: Ping the CPE from the CMTS to update the CM/ CPE association.</p>
CSCs198243	<p>Syslog messages are logged on the syslog server using one of the Gigabit Ethernet interfaces instead of the specified loopback interface.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(21a) BC3.</p> <p>Workaround: Reapply the <b>no logging source-interface Loopback0</b> and <b>logging source-interface Loopback0</b> commands.</p>

**Table 41** Open Caveats for Cisco IOS Release 12.3(23)BC1 (continued)

DDTS ID Number	Description
CSCsm08382	<p>When using the aggregate <code>cdxIfCmtsServiceOutOctets</code> MIB variable to obtain downstream byte counter statistics, some modems report a zero value for the downstream byte counter aggregate MIB.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3 (17b) BC4 or 12.3 (21a) BCx.</p> <p>From DOCSIS 1.1 onwards, statistics are maintained for each service flow, instead of the Service ID, in the DOCS-QOS-MIB in <code>docsQosServiceFlowStatsTable</code> objects. For cable modems not running in DOCSIS 1.0 mode, the objects <code>cdxIfCmtsServiceOutOctets</code> and <code>cdxIfCmtsServiceOutPackets</code> will only support primary service flow.</p> <p>There are no known workarounds.</p>
CSCsm12010	<p>In a uBR10012 router, packets sent from the cable modems to some Customer Premise Equipments (CPE) are lost due to possible hardware ARP information.</p> <p>This is observed when 2000 or more wideband modems are connected to a uBR10012 router.</p> <p>Workaround: Run <b>clear ip arp &lt;mac-address&gt;</b> command to get a new IP address.</p>
CSCsm15646	<p>When the CMTS is configured with more than 32 wideband groups, the wideband interface counters stop updating even with continuous traffic flow.</p> <p>Workaround: It is better to configure less than 32 Wideband interfaces.</p>
CSCsm19648	<p>A sharp decrease in the unicast traffic is observed when when configuring or un-configuring PIM on a Gigabit Ethernet interface.</p> <p>There are no known workarounds.</p>
CSCsm23260	<p>Timeout occurs when an Inter-Process Communication (IPC) request to the line card is blocked. The following message is displayed.</p> <pre>%REQGRP-3-SYSCALL: System call for command 42 (slot5/0) : Could not send blocked IPC message (Cause: timeout)</pre> <p>This issue is seen only on different cards that handle more than hundreds of modems.</p> <p>Workaround: Reload the card.</p>
CSCsm31562	<p>Cable modems do not return to online state when an operator executes a <b>shut/no-shut</b> command on the protect interface or resets the Protect linecard even after the Protect linecard comes up. This is observed on a uBR10000 router when the Protect linecard is active while the Working linecard is down.</p> <p>Workaround: If the Working linecard is brought back up in the standby mode, then the modems do come online on the Protect linecard.</p>
CSCsm33336	<p>Output of the <b>show controller cable x/x/x</b> command displays previous entries of narrowband (NB) channel when its <i>channel-id</i> is changed. However it does not impact the modem registration.</p> <p>Workaround: Do not change the <i>channel-id</i> value of the NB channel after configuration.</p>

**Table 41** Open Caveats for Cisco IOS Release 12.3(23)BC1 (continued)

DDTS ID Number	Description
CSCsm47906	<p>Cable modems drop offline when pre-equalization is enabled. This is also observed when a severe noise is found on the hybrid fiber-coaxial (HFC) system.</p> <p>Workaround: Disable and re-enable pre-equalization. In other words, execute:  <b>no cable upstream 0 equalization-coefficient</b>  <b>cable upstream 0 equalization-coefficient</b></p>
CSCsm49763	<p>On a uBR10012 router with PRE2, NetFlow does not detect traffic for PXF switched packets.</p> <p>There are no known workarounds.</p>
CSCsm52420	<p>On a Cisco uBR10000 series (PRE2) router, RP processor fails over by bus error crash, resulting in the router switching over to the standby RP.</p> <p>There are no known workarounds.</p>
CSCsm54577	<p>The following Fan Tray missing error occurs.</p> <pre>Oct 17 22:12:47.869: %UBR10K_ALARM-6-INFO: ASSERT CRITICAL fan-tray-slot Fan tray missing Oct 17 22:12:47.869: %CI-1-NOFAN: Fan tray empty Oct 18 05:47:23.287: %UBR10K_ALARM-6-INFO: CLEAR CRITICAL fan-tray-slot Fan tray missing Oct 18 05:47:23.287: %CI-6-BLOWEROK: Fan tray module OK</pre> <p>Workaround: Replacement of the Fan module does work in a few instances.</p>
CSCsm55512	<p>Tracebacks occur every time when INVALIDSIDPOSITION error is displayed in a CMTS that has a large number of cable modems with a few going offline.</p> <p>There are no known workarounds.</p>
CSCsm55957	<p>The Channel Grouping Domain (CGD) configuration does not work correctly on the Protect linecard after the linecard reverts and the working linecard takes over.</p> <p>Workaround: It is recommended to not make changes to the CGD on the Protect LC.</p>
CSCsm58028	<p>In the uBR10000 series router, alignment tracebacks and corrections in list enqueue and remove functions may be observed on the cable linecard during linecard N+1 switchover.</p> <p>This is usually seen after several Linecard switchovers and reverts along with PRE switchovers.</p> <p>There are no known workarounds.</p>
CSCsm64439	<p>The chassis serial number is not displayed when the <b>show inventory</b> command is run on the router.</p> <p>This observation is found on a uBR10000 (PRE1-RP) router.</p> <p>There are no known workarounds.</p>

**Table 41** *Open Caveats for Cisco IOS Release 12.3(23)BC1 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsm65883	<p>Modems do not go online on P after a linecard failover from W to P when the keepalive failure is already configured. Modems also do not go online on W after a revertback from P to W.</p> <p>This issue is observed only when another linecard failure occurred before the triggered keepalive linecard failover.</p> <p>There are no known workarounds.</p>
CSCsl35163	<p>The range-backoff configuration value changes from "range-backoff 3 6" to "range-backoff automatic" for upstream in a frequency stacking scenario.</p> <p>This change is noticed after the following commands are executed to un-configure and re-configure the cable interface:</p> <ol style="list-style-type: none"> <li>1. <b>cable upstream max-ports 6</b></li> <li>2. <b>no cable upstream max-ports</b></li> <li>3. <b>cable upstream max-ports 6</b></li> </ol> <p>Workaround: There is no workaround.</p>
CSCsl49206	<p>If the associated HA <b>ip host</b> commands are removed followed by PRE switchovers from PREA to PREB and then from PREB to PREA. After re-configuring the Global HA commands, all modems disappear, re-range and then come back online.</p> <p>There are no known workarounds.</p>
CSCsl72179	<p>Issuing the <b>shut</b> and <b>no shut</b> command stream causes PXF crash resulting in the "TBB Length" error.</p> <p>This is a rare occurrence.</p> <p>There are no known workarounds.</p>
CSCsl74859	<p>If the <b>show cable modem</b> command is used after a PRE switchover, cable modems are duplicated with the same MAC address.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(00)BC3.</p> <p>There are no known workarounds.</p>
CSCsd11861	<p>Jitter and latency occurs in specific UGS upstream service flows that use LLQ scheduling mode instead of the docsis compliant scheduling mode.</p> <p>This is observed when the upstream LLQ scheduling mode is enabled.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(23)BC1

Table 42 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(23)BC1.

**Table 42 Resolved Caveats for Cisco IOS Release 12.3(23)BC1**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsl73391	<p>CMTS sysUpTime parameter remains unchanged in IPDR document for all records thus making it unreliable for stop records. Similarly, IPDRcreationTime parameters are the same for interim records and are set to the data collection start time for the IPDR document. These may cause certain accounting issues.</p> <p>This issue occurs when Subscriber Account Management Interface Specification (SAMIS) feature is used.</p> <p>Workaround: Poll the DOCS-QOS-MIB object directly.</p>
CSCsl61201	<p>CMTS generates duplicate IPDR records for same service identifier (SID). This creates accounting issues for usage-based billing of cable modems.</p> <p>This issue occurs on uBR10012 and uBR7200 platforms running Cisco IOS Release 12.3(17b)BC4 when Subscriber Account Management Interface Specification (SAMIS) feature is used.</p>
CSCsd71318	<p>Cisco 2800 series router crashes when the connection to the URL filter server is reset, either due to network congestion or during a warm/cold reload.</p> <p>This bug also applies to Cisco uBR7100 series, uBR7200 series and uBR10012 universal broadband routers. This issue occurs with external Websense or N2H2 server.</p> <p>Workaround: There are no known workarounds for cold/warm reload. For crash due to network congestion or WAN reset, remove the condition that causes the connection to the URL filter to flap.</p>
CSCsk74962	<p>Router is experiencing spurious memory access while running the <b>show buffer assigned dump</b> command.</p> <p>This issue does not cause any operational problems.</p> <p>There are no known workarounds.</p>
CSCsh69471	<p>Symptom: AAA accounting requests are being sent with empty user name.</p> <p>Condition: This issue occurs while running the <b>show accounting</b> command for the affected accounting traffic.</p> <p>Workaround: No workaround is required as it is only a display issue.</p>
CSCsl32567	<p>When executing <b>show aaa attribute protocol radius</b> command, the router running Cisco IOS may crash or display junk characters.</p> <p>There are no known workarounds.</p>

Table 42 Resolved Caveats for Cisco IOS Release 12.3(23)BC1 (continued)

DDTS ID Number	Description
CSCs182266	<p>Loop occurs between uBR and CNR during <i>leasequery</i>. At the loop condition, you can see several leasequeries per second and after a while, the loop ends automatically.</p> <p>This issue occurs on following conditions:</p> <ul style="list-style-type: none"> <li>• <b>source-verify dhcp</b> is enabled.</li> <li>• CNR failover setup (Redundant CNR).</li> <li>• The target IP of the leasequery loop should be a CPE which is connected to currently offline CM and ARP entry for the CPE aged out.</li> </ul> <p>There are no known workarounds.</p>
CSCsk70446	<p>Traceback observed while using long URLs to configure a device using the Cisco IOS HTTP web parser.</p> <p>This issue occurs while trying to configure commands that have a single keyword or parameter greater than N characters in length, where N is:</p> <ul style="list-style-type: none"> <li>• 50 for Cisco IOS Release 12.0 and above</li> <li>• 128 for Cisco IOS Release 12.2 and above</li> <li>• 256 for Cisco IOS Release 12.2(25) and above</li> </ul> <p>Workaround: Avoid using the Cisco IOS HTTP web parser for commands with long keywords or arguments.</p>
CSCdx17766	<p>Alarm message is not getting cleared after PRE cutover.</p> <p>Workaround: Use the <b>show redundancy</b> command to see the true state of the redundant PRE.</p>
CSCeh97270	<p>HA code on PRE2 is not monitoring Linecard and Backplane Ethernet (BPE) health. As a result, proper switchovers are not taking place when issues arise. It leads to forwarding issues that require manual intervention.</p> <p>There are no known workarounds.</p>
CSCsg50812	<p>Symptom: Multicast traffic is dropped by the Half Height Gigabit Ethernet (HHGE) or Full Height Gigabit Ethernet (FHGE) linecards when links of an EtherChannel port are bounced by the <b>shutdown</b> or <b>no shutdown</b> command causing the OSPF neighbor not going into full state.</p> <p>Workaround: Use the <b>shutdown</b> or <b>no shutdown</b> command at the aggregate Ethernet Channel port.</p>
CSCsm45454	<p>All cable modems on the same SPA card remain offline. This issue occurs when the downstream control message queue is stuck due to a race condition.</p> <p>Workaround: Disable the Dynamic Bandwidth Selection (DBS) feature.</p>
CSCsj97439	<p>The <b>clear cable host vrf xxx</b> command is not working correctly for bundle interface with multiple subinterfaces belonging to different VRFs.</p> <p>Workaround: Use VRF of the cable modem (VRF sid in) to clear the host. For example, if the CM has sid 10 in VRF RED and two CPEs behind the CM are in VRF BLUE and GREEN, use the sid VRF RED to remove the CPEs (<b>clear cable host VRF RED xxx.xxx.xxx.xxx</b>).</p>

Table 42 Resolved Caveats for Cisco IOS Release 12.3(23)BC1 (continued)

DDTS ID Number	Description
CSCsk36491	<p>Changing the bonding group ID on a wideband interface prevents the wideband cable modems on that interface from being marked offline after the interface goes down.</p> <p>Workaround: Reset modems on that interface (bonding group) one by one. This will bring back the modems online with the correct (new) bonding group ID. You can also try the <b>clear cable modem all reset</b> command.</p>
CSCsk39347	<p>During the Online Insertion and Removal (OIR) process in an HA WORKING line card, all modems failover to the PROTECT mode, resulting in a loss of the PCMM gates or test PacketCable. However, the dynamic service flows and PCMM voice calls function normally.</p> <p>There are no known workarounds.</p>
CSCsk41966	<p>On an uBR10k running 12.3(21a)BC2, the interface mac-scheduler reports higher number of active UGS flows than active calls reported by "show calbe calls" for that interface. It also holds the UGS flow BW and do not release. UGS flows are NOT stuck though.</p> <p>The following is an example:</p> <pre>show cable calls reports 2 active UGS calls while mac-scheduler reports 17.</pre> <pre>Router#sh cable modem calls   i 8/1/2/U0 0011.e3ef.6e3d 10.66.50.91 C8/1/2/U0 4029 V - 0011.e3ec.cee2 10.66.52.184 C8/1/2/U0 2143 V</pre> <pre>Router#sh int c8/1/2 mac-scheduler 0 &lt;snip&gt;</pre> <pre>ched Table Adm-State: Grants 17, Reqpolls 0, Util 19% UGS : 17 SIDs, Reservation-level in bps 1543600</pre> <p>Router#</p> <p>This issue is only observed when DS load balancing is enable and only on the USs, which are a part of the LB group.</p> <p>There are no known workarounds.</p>
CSCsk53235	<p>If config ip access-group in on a cable bundle interface, then delete this interface using the <b>no interface bundle n</b> command. Then recreate the bundle interface, configure ip access-group in on the interface and the traceback appears.</p> <p>This issue is seen in a uBR10k running 12.3(23)BC.</p> <p>There are no known workarounds.</p>
CSCsk63745	<p>Reduced downstream throughput occurs over time on uBR10k routers with &gt;40000 modems.</p> <p>BE queue aggregation must be taking place for this problem to occur.</p> <p>There are no known workarounds.</p>

**Table 42 Resolved Caveats for Cisco IOS Release 12.3(23)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsl09172	<p>The <b>show inventory</b> command does not provide the secondary Performance Routing Engine (PRE) serial number.</p> <p>Workaround: Enable the <b>secondary console enable</b> hidden command before logging into the secondary console and then run the command to obtain secondary PRE serial number.</p>
CSCsl19255	<p>Pre-allocated queues do not get preallocated for downstream interfaces above 40. This could potentially create an issue for newly created interfaces in the event that the router is undergoing BE queue aggregation. The symptom would be that if the router was undergoing BE queue aggregation and new interfaces were added to the configuration, modems could fail to come online on the newly created interfaces.</p> <p>The condition exists when there are more than 40 downstream interfaces. Prior to this release the maximum number of downstream interfaces that could be provisioned on the uBR10k was 40. Support for Modular Cable and Wideband Cable increases this maximum to greater than 40. The infrastructure fails to provide pre-allocated queues for newly created downstream interfaces.</p> <p>Workaround: The workaround would be to provision new interfaces, when the new downstream interfaces would increase the total number of downstream interfaces to greater than 40, and then reload the router.</p>
CSCsl29160	<p>Running the <b>unconfig hccp</b> command on linecard generates ALIGN-3-TRACE tracebacks.</p> <p>There are no known workarounds and it will not cause any service disruption.</p>
CSCsl32472	<p>Cable Modems receive one-third to one-fourth of the bandwidth on few downstreams. However, not all downstreams on the Cisco uBR10-MC5X20U linecard are affected, except some upstreams.</p> <p>This issue occurs on uBR10k running Cisco IOS Release 12.3(21a) BC1 with 520u cards.</p> <p>Workaround: Reload the parallel express forwarding (PXF).</p>
CSCsl40446	<p>The cmts uses the wrong rf-switch snmp community string during a LC switchover from W to P. As a consequence, once the modems failover to the PROTECT card, they fall offline and never come online. This issue is seen after configuring a rf-switch snmp community string, followed by PRE failovers from PREA to PREB and then back from PREB to PREA and then removing the configured rf-switch snmp community string.</p> <p>There are no known workarounds.</p>
CSCsl40777	<p>Traceback is observed when <b>no cable rf-bandwidth-percent</b> command is issued for MC interface. This issue occurs when CIR queues are configured for modems.</p> <p>There are no known workarounds.</p>
CSCsl42722	<p>WCMs go offline while NCMs remain online after a PRE switchover.</p> <p>There are no known workarounds.</p>
CSCsl44111	<p>The <i>ifName</i> (textual interface name) displayed for bundle subinterface is not CNEM compliant.</p> <p>There are no known workarounds.</p>

Table 42 Resolved Caveats for Cisco IOS Release 12.3(23)BC1 (continued)

DDTS ID Number	Description
CSCs151718	<p>The MC interface parameter changes occurred after an LC switchover is getting lost when the LC reverts back.</p> <p>Workaround: Update the MC interface parameters after the LC reverts back.</p>
CSCs154498	<p>IPC timeout error messages and tracebacks are experienced on cable linecards after issuing <b>ip telnet source-interface loopback</b> and <b>if-console</b> commands on the CMTS.</p> <p>This issue has been seen on a UBR10012 platform running IOS 12.3(17b)BC6.</p> <p>Workaround: Reset the linecards generating the errors using <b>hw-module reset</b> or rebooting the CMTS resolves the issue.</p>
CSCs157861	<p>OIR removal of the DOCSIS downstream SPA will cause modems using the modular downstreams of the other SPA to go offline.</p> <p>The PXF queues used for MAP traffic are stuck and have continuous tail drops. The MAP queue id for a SPA can be found in <b>show pxf cpu queue wb-spa</b> command.</p> <p>Heavy load (data and DOCSIS MAC management traffic including MAPs) on the SPA jacket card increase the chances of running into this issue</p> <p>Workaround: Stop all traffic to the SPA before the OIR removal by shutting down all the Modular-Cable and Wideband interface associated with the SPA.</p> <p>If the interfaces are not shutdown then reset Saratoga Jacket card if these symptoms occur after the SPA OIR.</p>
CSCs169376	<p>After two or more of PRE switchovers by the admin for IOS upgrade, all CMs connected to the systems will encounter download speeds less than 1Mbps.</p> <p>This issue occurs whenever two or more PRE switchovers are executed. This error occurred in 12.3(17b)BC3 and BC5. When tested in 12.3(13a)BC3 and 12.3(21)BC, there was no problem.</p> <p>Workaround: Performing a CM disconnect and reconnect solves this problem.</p>
CSCs172511	<p>Some configuration steps on an RF channel's annex and/or modulation is not making the Wideband Cable interface operational.</p> <p>This issue occurs when the user deletes the RF channel's configuration about annex and/or modulation by <b>no rf-channel n frequency annex A B modulation 64qam 256qam interleave</b> command and then configures the RF channel as Annex B and 64QAM. If the same steps are repeated on all RF channels of a Wideband Cable interface, then no modems can come w-online on this interface as it will not be operational.</p> <p>Workaround: Configure the problematic RF channel as Annex A and/or 256QAM, and then revert to the desired configuration.</p>
CSCs173846	<p>A Modular Cable interface may result in an unexpected behavior after a quick <b>shutdown</b> and <b>no shutdown</b>.</p> <p>Workaround: After shutting down a Modular Cable interface, wait for at least five seconds before proceeding with any further configuration.</p>

**Table 42** *Resolved Caveats for Cisco IOS Release 12.3(23)BC1 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCs174050	<p>Unable to ping the w-online modem when the committed information rate (CIR) is very high.</p> <p>Workaround: Ensure that the CIR of WCM service flows is less than the CIR of the WB interface.</p>
CSCs177607	<p>Upstream cable filter groups for CM and CPE types do not work. ACLs created by the filter group look correct, but does not block qualifying upstream traffic.</p> <p>This issue is also seen in 12.3(21a)BC4. Downstream filter groups work fine for both CM and CPE types.</p> <p>There are no known workarounds.</p>
CSCs189471	<p>WB modem does not change to wideband-online status after adding <b>modular-host subslot</b>.</p> <p>This problem is seen when <b>modular-host subslot</b> is configured on any modular controller and FN is configured instead of Channel Grouping Domain (CGD).</p> <p>Workaround: Configure CGD before adding <b>modular-host subslot</b>.</p>
CSCs190289	<p>When the dynamic interleaver (via the upstream modulation profile) is enabled on the MC5x20H BPE line card all cable modems go offline after several hours.</p> <p>There are no known workarounds.</p>
CSCs191048	<p>The <b>show tech-support</b> and <b>show cable tech-support</b> commands do not provide information about <b>modular-cable x/y/z</b> and <b>jacket x/y</b> in privileged EXEC mode.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(21a) BC3.</p> <p>Workaround: Manually collect the following data:</p> <ul style="list-style-type: none"> <li>• Show controller jacket x/y</li> <li>• Show controller modular-cable x/y/z</li> </ul>
CSCsm14437	<p>In rare occasions, a service flow with minimal reserved rate requirement may get admitted but no traffic can be sent over it.</p> <p>There are no known workarounds.</p>

**Table 42** *Resolved Caveats for Cisco IOS Release 12.3(23)BC1 (continued)*

DDTS ID Number	Description
CSCsm24599	<p>The SA and Cooper modem firmware is not sending RCP when MDD is not detected. It breaks the existing CMTS logic to identify a WB-capable modem and corresponding DS channel selection features. These features are intended to move a WB-capable modem to a bonded primary channel or a non-bonding capable channel to a non-bonded primary channel.</p> <p>Workaround: Change the settings of the WB-capable modem to meet one of the following conditions:</p> <ul style="list-style-type: none"> <li>• RCP is reported in the modem REG-REQ and known to CMTS.</li> <li>• No RCP is reported. However, the modem's Receive Tuner Capacity should be &gt;1 and no unknown RCP should be reported during previous registration attempts. You can also issue &lt;clear cable modem non-bonding-capable delete&gt; command to clean up the modem's previous unknown RCP index. It allows the modem to be treated as WB-capable modem on a DS channel without MDD and helps the modem to register itself with an RCP recognizable by the CMTS, even if there is a change in firmware.</li> </ul>
CSCsm42787	<p>Adding new upstreams to a primary modular RF channel in a Channel Grouping domain overwrites the previously configured upstreams and brings the modems using those upstreams to offline status.</p> <p>Workaround: To add 0-1 upstreams in a channel already configured with 2-3 upstreams, use the <b>downstream modular-cable 1/0/x rf-channel x upstream 0-3</b> command. It will keep the previously configured upstreams (2-3) while adding the new ones.</p>
CSCsi69299	<p>Error messages end up in the crashinfo file of the PRE that is going down. The issue occurs under some PRE switchover scenarios, for both c10k and uBR10k, where 'process_may_suspend' is called within interrupt context.</p> <p>There are no known workarounds.</p>
CSCsk03915	<p>The uBR10000 series router is not filtering some cable downstream packets. The issue is observed for IPv4 packets. The packets are sent from CMTS to CM/CPE and the downstream cable filters configured in the PRE2 of the router fails to filter it. However, it does not affect the functionality of the router and the packets from external sources are filtered as expected.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(21a)BC6

Table 43 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC6.

**Table 43**      **Open Caveats for Cisco IOS Release 12.3(21a)BC6**

DDTS ID Number	Description
CSCsl73391	<p>CMTS sysUpTime parameter remains unchanged in IPDR document for all records thus making it unreliable for stop records. Similarly, IPDRcreationTime parameters are the same for interim records and are set to the data collection start time for the IPDR document. These may cause certain accounting issues.</p> <p>This issue occurs when Subscriber Account Management Interface Specification (SAMIS) feature is used.</p> <p>Workaround: Poll the DOCS-QOS-MIB object directly.</p>
CSCsl61201	<p>CMTS generates duplicate IPDR records for same service identifier (SID). This creates accounting issues for usage-based billing of cable modems.</p> <p>This issue occurs on uBR10012 and uBR7200 platforms running Cisco IOS Release 12.3(17b)BC4 when Subscriber Account Management Interface Specification (SAMIS) feature is used.</p>
CSCsi46184	<p>IOS crashes, when you remove a PCMCIA card that is in use.</p> <p>Workaround: Do NOT remove the flash card when it is in use.</p>
CSCek41611	<p>Cisco uBR10-MC5X20U cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>
CSCek66377	<p>Not all entries are seen for the Protect line card in the MIB table.</p> <p>There are no known workarounds.</p>
CSCsl74859	<p>If the <b>show cable modem</b> command is used after a PRE switchover, cable modems are duplicated with the same MAC address.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(00)BC3.</p> <p>There are no known workarounds.</p>
CSCek77620	<p>This issue is fixed in 12.3(21)BC4 release through CSCsj31345.</p> <p>Workaround: If you cannot ping modems, try using the <b>clear cable modem reset</b> command and retry running ping for modems.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>

**Table 43**      **Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)**

DDTS ID Number	Description
CSCsd14355	<p>The Simple Network Management Protocol (SNMP)-created quality of service (QoS) profile is not available after a Performance Routing Engine (PRE) switchover; the command- created QoS profile is available after switchover.</p> <p>There are no known workarounds.</p>
CSCsl79007	<p>Memory corruption at input/ output (I/O) memory occurs due to a redzone overrun, causing a PRE2 switchover.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17b) BC5.</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsl80817	<p>When making a voice call with data traffic saturation in upstream and downstream directions, the voice call packets-per-second (PPS) value is reduced to less than 49.</p> <p>The expected PPS is 49 or 50 after polling for a specific duration.</p> <p>There are no known workarounds.</p>
CSCsh19917	<p>Some parent warnings appear when static analysis is performed on the specmib source file.</p> <p>Workaround: No workaround is required. The functionality of the MIB query is not affected.</p>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li data-bbox="574 1270 1474 1396">1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachables" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li data-bbox="574 1417 1474 1501">2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachables" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh41508	<p>The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.</p> <p>There are no known workarounds.</p>

**Table 43** Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)

DDTS ID Number	Description
CSCs189471	<p>WB modem does not change to wideband-online status after adding <b>modular-host subslot</b>.</p> <p>This problem is seen when <b>modular-host subslot</b> is configured on any modular controller and FN is configured instead of Channel Grouping Domain (CGD).</p> <p>Workaround: Configure CGD before adding <b>modular-host subslot</b>.</p>
CSCsh66150	<p>The <b>show cable modem connectivity</b> command output is corrupted under some condition.</p> <p>The following example shows a sample output.</p> <pre> ----- show cable modem connectivity ----- Prim 1st time   Times %online   Online time           Offline time Sid  online      Online      min   avg   max   min   avg max 9    04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 11   04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 </pre> <p>This issue occurs after PRE switchover.</p> <p>Workaround: Clear cable modem delete.</p>
CSCsh69870	<p>The VTMS algorithm has to be optimized due when CMs with different MIRs are mixed. The Downstream can not be fully utilize by a CM configured with a very high MIR (16-20Mbps), even when there is BW available in such Downstream.</p> <p>There are no known workarounds.</p>
CSCsh70679	<p>When sending a trap due to exceeding a threshold, the admission control system fails to report the correct type of event that triggered the threshold to be exceeded.</p> <p>There are no known workarounds.</p>
CSCsh72785	<p>No SNMP trap is generated on behalf of the redundant PRE state change.</p> <p>This issue may occur on the redundant PRE configuration and state change of redundant unit.</p> <p>There are no known workarounds.</p>
CSCsh95096	<p>On a Cisco uBR10012 running Cisco IOS Release 12.3(21)BC, it is possible to change default connector commands even if modems are online on that upstream connector.</p> <p>There are no known workarounds.</p>
CSCsh96105	<p>Under the following conditions, tracebacks are seen and the modem does not come online.</p> <ul style="list-style-type: none"> <li>• HCCP is configured and activated.</li> <li>• A modem changes upstream to an DOCSIS 2.0 only channel.</li> </ul> <p>Workaround: Delete the modem and let it come online again.</p>

**Table 43** Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)

DDTS ID Number	Description
CSCsi05236	<p>When the Ubr10k Half-Height GE linecard is connected to the SCE2000 GE link and both are configured with auto-negotiation, the link does not come up. This problem does not exist for the Full-Height GE.</p> <p>This issue occurs when an Ubr10k Half-Height GE is directly connected to the SCE GE link and auto-negotiation is turned on both links.</p> <p>Workaround: If the auto-negotiation is removed from both GE interfaces, then the link will come up.</p>
CSCsi09848	<p>Pagent cannot get a predefined IP DHCP pool so it will automatically be assigned the default. (192.168.100.x).</p> <p>This issue occurs when running HA regression cases.</p> <p>Workaround: Rerun the case.</p>
CSCsi27520	<p>The following interface RPF configuration commands are accepted on theubr10k even though they are not supported in theubr10k microcode:</p> <p><b>ip unicast source reachable-via any allow-default</b></p> <p><b>ip unicast source reachable-via rx &lt;1-199&gt;</b></p> <p><b>ip unicast source reachable-via rx &lt;1300-2699&gt;</b></p> <p>Workaround: Do not configure the unsupported commands.</p>
CSCsi33625	<p>The code automatically changes the acceptable upstream (US) power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This setting is legal for all US channel width options.</p>
CSCsi41787	<p>The <b>show int if downstream</b> CLI shows “cable interface downstream is up” even though the interface is in shutdown state.</p> <p>There are no known workarounds.</p>
CSCsi91048	<p>The <b>show tech-support</b> and <b>show cable tech-support</b> commands do not provide information about <b>modular-cable x/y/z</b> and <b>jacket x/y</b> in privileged EXEC mode.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(21a) BC3.</p> <p>Workaround: Manually collect the following data:</p> <ul style="list-style-type: none"> <li>• Show controller jacket x/y</li> <li>• Show controller modular-cable x/y/z</li> </ul>

**Table 43** *Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsi96432	<p>The association between a customer premises equipment (CPE) and a cable modem (CM) is lost after an N+1 switchover even though the host route determined by the Routing Information Protocol (RIP) appears in the VPN routing/forwarding (VRF) table.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a) BC2.</p> <p>Workaround: Ping the CPE from the CMTS to update the CM/ CPE association.</p>
CSCsi48608	<p>ACL configured to the CPE is not available after line card/interface switchover.</p> <p>This issue occurs when using <b>cable {modem   host   device} access-group acl</b>.</p> <p>Workaround: Reconfigure ACL to the CPE manually after switchover.</p>
CSCsi98243	<p>Syslog messages are logged on the syslog server using one of the Gigabit Ethernet interfaces instead of the specified loopback interface.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(21a) BC3.</p> <p>Workaround: Reapply the <b>no logging source-interface Loopback0</b> and <b>logging source-interface Loopback0</b> commands.</p>
CSCsm08382	<p>When using the aggregate <code>cdxIfCmtsServiceOutOctets</code> MIB variable to obtain downstream byte counter statistics, some modems report a zero value for the downstream byte counter aggregate MIB.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3 (17b) BC4 or 12.3 (21a) BCx.</p> <p>From DOCSIS 1.1 onwards, statistics are maintained for each service flow, instead of the Service ID, in the DOCS-QOS-MIB in <code>docsQosServiceFlowStatsTable</code> objects. For cable modems not running in DOCSIS 1.0 mode, the objects <code>cdxIfCmtsServiceOutOctets</code> and <code>cdxIfCmtsServiceOutPackets</code> will only support primary service flow.</p> <p>There are no known workarounds.</p>
CSCsi81513	<p>HCCP status shows that everything is synced and the Protect is ready for switchover, even though nothing has been synced over and the interdb on the Protect LC is empty.</p> <p>A LC switchover after this is totally broken and modems will never register on the Protect LC</p> <p>This happens only when the Blaze FPGA image is changed for the Modena and is being reprogrammed on CMTS bootup.</p> <p>Workaround: The modems will not register on the modular interface when Blaze FPGA is being reprogrammed. As soon as the Blaze is reprogrammed, reload the CMTS as the modems are already down.</p> <p>On reload everything should work correctly.</p>

**Table 43** Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)

DDTS ID Number	Description
CSCsi85054	<p>When dynamic cable modem load balancing is configured between downstream A and downstream B, and downstream B's service flow admission control thresholds are significantly lower than downstream A's. It appears that load balancing still moves modems across to downstream B, even after violating the prescribed Admission control limits.</p> <p>There are no known workarounds.</p>
CSCsi87195	<p>When you configure frequency using SNMP, the range of frequencies accepted is based on the following formula.</p> $\text{min\_us\_freq} = 5000000 + (\text{channel\_width}/2)$ $\text{max\_us\_freq} = 55000000 - (\text{channel\_width}/2)$ <p>Given a frequency configured, when configuring a channel width that cannot accept the frequency configured already, there should be warning message saying that "channel width cannot be configured with the present frequency".</p> <p>This problem occurs when the frequency you are trying to configure via SNMP is not within the channel width currently configured on the CMTS router.</p> <p>There are no known workarounds.</p>
CSCsj12497	<p>When the <b>cable per-dev-acl</b> command is configured, the access-list assigned to the host is not available after a PRE switchover.</p> <p>There are no known workarounds.</p>
CSCsj58093	<p>CPE ping stops after the wideband (WB) switches to the narrowband (NB) mode.</p> <p>This problem occurs when you shut down the WB interface.</p> <p>Workaround: Execute <b>clear arp</b> or <b>clear cable modem</b> commands to clear the ARP entries and then let the cable modem on the NB to come online.</p>
CSCsj64207	<p>It seems that the total downstream rate applied to Annex A 256QAM downstreams by admission control is only 1543127 bits per second, as opposed to the real rate which is somewhere around 50Mbps.</p> <p>There are no known workarounds.</p>
CSCsj84440	<p>Adding an RF channel to a WB interface, by configuring <b>cable rf-channel</b> under wideband-cable interface, will cause the corresponding wideband modems to leave w-online state with a "Fiber node x status changed to Invalid state" message shown in CLI.</p> <p>If the RF channel is currently in a fiber node and it is also used by a WB interface, and the fiber node is in a "Valid" state. If this RF channel is added to a new WB interface that does not yet have bundle configured (or a different bundle configured), the fiber node will become "Invalid" due to mismatched bundle number. This will cause the failure of the MD-DS-SG creation and thus WB modem offline.</p> <p>Workaround: Avoid adding a RF channel to a WB interface with a different bundle configuration than the existing one.</p>
CSCsk07617	<p>The <b>show cable modem qos</b> command incorrectly shows the original ToS mask after overwrite.</p> <p>There are no known workarounds.</p>

**Table 43** *Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsk10852	RF channel mismatch error occurs when you run the <b>show hw-module bay association wideband-channel</b> command.  There are no known workarounds.
CSCsk12224	After LC switchover, modems cannot be assigned with any CM-created DOCSIS 1.0 QoS profile. The <b>cable modem qos profile</b> command works but the profile does not get assigned  The defect is seen in all software releases.  Workaround: Delete the modem before assigning the CM-created QoS profile using the <b>clear cable modem delete</b> command.
CSCsk20304	When using the <b>show cable bundle</b> command with traffic going to a CPE device behind a wideband cable modem, the data going to the CPE is not seen on the bundle interface that it is using. This data will appear on the input GE port and the wideband interface.  There are no known workarounds.
CSCsk28938	On a uBR10k running 12.3(17a)BC and up (and older code, as well), the <b>cable downstream rate-limit</b> command has no affect on DS traffic.  There are no known workarounds.
CSCsk39347	During the Online Insertion and Removal (OIR) process in an HA WORKING line card, all modems failover to the PROTECT mode, resulting in a loss of the PCMM gates or test PacketCable. However, the dynamic service flows and PCMM voice calls function normally.  There are no known workarounds.
CSCsk41698	In the following scenario, if a customer mistakenly configures LC 5/0 as PROTECT, plus the <b>no mem sub x/y revertive</b> command and then corrects the problem by configuring LC 5/1 as PROTECT, the <b>no mem sub x/y revertive</b> command is not reflected in the <b>show hccp detail</b> output.  Workaround: Reconfigure the <b>no mem sub x/y revertive</b> command.
CSCsk53180	The output of <b>show controllers cx/y/z tech-support</b> contains passwords in the running-configuration. These passwords should be removed, as these tech-support reports are routinely sent to TAC via non-secure email.  There are no known workarounds.
CSCsk65431	Changing IP add on the int bundle X.1 subinterface results in an Integrated Up-converter flap for all interfaces associated with that bundle.  This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17)BC or higher that has a bundle interface configured.  There are no known workarounds.
CSCsk68026	Bus error exception crash on PRE of uBr10k.  This issue occurs on an uBr10k with IOS 12.3(21a)BC2, seen on PRE1 as well as PRE2.  There are no known workarounds.

**Table 43**      **Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsk72430	<p>Increasing docsis frag header discard counters are seen in 12.3(21a)BC3 when running US at high utilization rate. This problems affect multiple CMs.</p> <p>Workaround: Disable docsis frag.</p>
CSCsl06036	<p>Maxcpe functionality is broken with w-online modems. The functionality is working with the same modem in the same image when it registered in the online state.</p> <p>There are no known workarounds.</p>
CSCsl10231	<p>A downstream service flow with an associated classifier will have the classifier “match count” initialized to zero if there is a PRE switchover or a reload of the pxf.</p> <p>This issue occurs on a service flow with a classifier and PRE switchover or pxf reload.</p> <p>There are no known workarounds.</p>
CSCsl26209	<p>uBR10000 with PRE2 reports inconsistent (much lower) input byte rate and packet rate than directly attached device over GE interface.</p> <p>The issue appears to be cosmetic affecting traffic counters only. This is observable only when GE interface has 802.1q tagged subinterfaces configured.</p> <p>There are no known workarounds.</p>
CSCsl37665	<p>Since the service flow is not in active state, “cable service flow activity-timeout 1800” will not help. Another timer which is “Admitted QoS timer” should have kicked in and cleaned it. Since that did not happen it is still an issue.</p> <p>There is no equivalent command to clean out service flows in admitted state.</p> <p>Customer has a a non-packet VOIP service, and currently have the activity-timeout set to 1800 seconds (implemented about 4 months ago) this value is what is being placed as the Active QoS timeout.</p> <p>Workaround: Try clearing the Cable Modem using the command <b>clear cable modem</b>. If there are many flows, you could also try to script it.</p>
CSCsl42554	<p>All CMs became offline with no alert or log message. When <b>clear cable modem all delete</b> command was executed, no CM was ranging. When checked, upconverter signal was ok and ucd counter also normal.</p> <p>This issue is observed in routers with the Cisco MC520H linecard.</p> <p>Workaround: Use <b>cable downstream rf-shutdown</b> and <b>no cable downstream rf-shutdown</b> commands.</p>
CSCsl42777	<p>Traceback observed in <code>cmts_cgd_get_active_primary</code> on the secondary PRE when image is upgraded resulting in a SPA FPGA upgrade.</p> <p>Modular cable interfaces are configured with the 12.3(23)BC and associated with a “Channel Grouping Domain” using the <b>downstream modular-cable interface</b> command.</p> <p>There are no known workarounds.</p>

**Table 43** Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)

DDTS ID Number	Description
CSCsl43172	<p>Traceback observed during cable linecard switchover on the linecard becoming active.</p> <p>Modular cable interfaces are configured and associated with a “Channel Grouping Domain” using the <b>downstream Modular-Cable</b> interface command.</p> <p>There are no known workarounds.</p>
CSCsl43380	<p>After multiple interfaces on different 520 linecards switchover and then revert, UBR10K-6-CM-INCONSISTENCY messages may be seen for wideband modems, and those modems will flap.</p> <p>This problem affects 12.3BC(23) and is seen with the following conditions.</p> <ol style="list-style-type: none"> <li>1. HCCP is configured with interface commands.</li> <li>2. Interfaces on multiple linecards switchover.</li> <li>3. One or more interfaces that switchover are on a linecard that is the modular-host for a SPA.</li> </ol> <p>Workaround: This problem will not occur if HCCP is configured with global commands, which force all interfaces on a linecard to switchover.</p>
CSCsl45841	<p>Call drops and PSQM failures observed when making bulk packetcable calls.</p> <p>There are no known workarounds.</p>
CSCsl49206	<p>If the associated HA <b>ip host</b> commands are removed followed by PRE switchovers from PREA to PREB and then from PREB to PREA. After re-configuring the Global HA commands, all modems disappear, re-range and then come back online.</p> <p>There are no known workarounds.</p>
CSCsl50048	<p>Modems cannot register on modular-cable downstreams when they use config files that have downstream llq (max downstream latency) set, but do not have min and max DS rate configured.</p> <p>These modems are stuck in reject (c) state</p> <p>Workaround: Add min and max DS rate in the downstream service flow encoding in the configuration file.</p>
CSCsl57014	<p>An unexpected crash occurs when executing a <b>show ip interface brief</b> soon after load and bootup.</p> <p>There are no known workarounds.</p>
CSCsl57849	<p>Voice subs experience one way audio</p> <p>Workaround: Issue the <b>hw-module slot x stop/start</b> command.</p>

Table 43 Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)

DDTS ID Number	Description
CSCs157861	<p>OIR removal of the DOCSIS downstream SPA will cause modems using the modular downstreams of the other SPA to go offline.</p> <p>The PXF queues used for MAP traffic are stuck and have continuous tail drops. The MAP queue id for a SPA can be found in <b>show pxf cpu queue wb-spa</b> command.</p> <p>Heavy load (data and DOCSIS MAC management traffic including MAPs) on the SPA jacket card increase the chances of running into this issue</p> <p>Workaround: Stop all traffic to the SPA before the OIR removal by shutting down all the Modular-Cable and Wideband interface associated with the SPA.</p> <p>If the interfaces are not shutdown then reset Saratoga Jacket card if these symptoms occur after the SPA OIR.</p>
CSCs171939	<p>On a DOCSIS1.0 modem, multiple customer premises equipments (CPE) get IP addresses when the <b>max-cpe</b> value is set to 1.</p> <p>There are no known workarounds.</p>
CSCs172140	<p>Few modems, with similar configurations, were stuck in the <b>init(io)</b> state and could not proceed further.</p> <p>Workaround: Execute <b>clear cable modem [mac-address] delete</b> command.</p>
CSCs173846	<p>A Modular Cable interface may result in an unexpected behavior after a quick <b>shutdown</b> and <b>no shutdown</b>.</p> <p>Workaround: After shutting down a Modular Cable interface, wait for at least five seconds before proceeding with any further configuration.</p>
CSCs173926	<p>On a wideband SPA (Shared Port Adapter), when one SFP module is disconnected the other module does not connect as expected.</p> <p>There are no known workarounds.</p>
CSCs174050	<p>Unable to ping the w-online modem when the committed information rate (CIR) is very high.</p> <p>Workaround: Ensure that the CIR of WCM service flows is less than the CIR of the WB interface.</p>
CSCsk31357	<p>PCMM gates will not be synced to the standby RP. Hence, if there is a PRE switchover, the newly active RP will not have the PCMM gate information.</p> <p>This issue occurs when running config only has “packetcable multimedia” enabled but not “packetcable”.</p> <p>Workaround: Enable “packetcable” in running configuration.</p>
CSCsj12597	<p>As part of OSSI requirement, dot3StatsCarrierSenseErrors need to incremented when the cable is removed from FE Interface. However, this is not happening.</p> <p>There are no known workarounds.</p>

**Table 43** *Open Caveats for Cisco IOS Release 12.3(21a)BC6 (continued)*

DDTS ID Number	Description
CSCsk60014	<p>Symptom: No downstream throughput for PC calls on eMTA accompanied by a warning after a PRE failover. The problem occurs because the standby PRE fails to start its WBCMTS periodic timer after the failover. When the problem occurs wideband capable modems fail to come online in wideband mode and register as narrowband modems instead.</p> <p>Condition: The problem occurs if the failover happens before the Wideband SPA has reached its operational state. This could happen if the card was not inserted prior to the failover. This could also happen if the failover occurred concurrently with downloading the operational firmware. For example, it could happen if the active and standby PREs boot simultaneously and the active PRE is in the process of bringing up the WB SPA when a PRE failover occurs.</p> <p>Workaround: Reload the router.</p>
CSCsj14502	<p>In certain cases, CMTS does not send intercept packets out in case of cTapStreamIpInterface is set to -1, while other parameters are set correctly in cTapStreamIpTable and snmpwalk show the cTapStreamIpStatus is active.</p> <p>The issue occurs when configuring a cTapStreamIp entry as follows:</p> <pre> cTapStreamIpInterface = -1 cTapStreamIpDestinationAddress = Addr1 cTapStreamIpDestinationLength = 32 cTapStreamIpSourceAddress = Addr2 cTapStreamIpSourceLength = 32 </pre> <p>and Addr1 is directly connected to a cable interface, Addr2 is routed through another interface and the net mask of outgoing interface for destination Addr2 is greater than the one of Addr1.</p> <p>Workaround: Perform one of the following:</p> <p>(1) Directly set the tapping interface's IfIndex, letting cTapStreamIpInterface != -1 and != 0</p> <p>(2) or, Either set cTapStreamIpSourceAddress or cTapStreamIpDestinationAddress to zero, to avoid conflict.</p>

## Resolved Caveats for Release 12.3(21a)BC6

Table 44 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC6.

**Table 44 Resolved Caveats for Cisco IOS Release 12.3(21a)BC6**

DDTS ID Number	Description
CSCs190289	When the dynamic interleaver (via the upstream modulation profile) is enabled on the MC5x20H BPE line card all cable modems go offline after several hours. There are no known workarounds.
CSCsk85933	A uBR10k running 12.3(17b)BC3 may report Cable Modems stuck in init(rc) state on certain Upstream Interfaces. Very high number of Input queue drops are also observed under the corresponding Downstream interfaces. This problem has only been observed on uBR10K with MC5x20H-D card. Workaround: Reseating the line card will bring all the Cable Modems back to online.

## Open Caveats for Release 12.3(21a)BC5

Table 45 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC5.

**Table 45 Open Caveats for Cisco IOS Release 12.3(21a)BC5**

DDTS ID Number	Description
CSCs173391	CMTS sysUpTime parameter remains unchanged in IPDR document for all records thus making it unreliable for stop records. Similarly, IPDRcreationTime parameters are the same for interim records and are set to the data collection start time for the IPDR document. These may cause certain accounting issues. This issue occurs when Subscriber Account Management Interface Specification (SAMIS) feature is used. Workaround: Poll the DOCS-QOS-MIB object directly.
CSCs161201	CMTS generates duplicate IPDR records for same service identifier (SID). This creates accounting issues for usage-based billing of cable modems. This issue occurs on uBR10012 and uBR7200 platforms running Cisco IOS Release 12.3(17b)BC4 when Subscriber Account Management Interface Specification (SAMIS) feature is used.
CSCsi46184	IOS crashes, when you remove a PCMCIA card that is in use. Workaround: Do NOT remove the flash card when it is in use.
CSCek41611	Cisco uBR10-MC5X20U cards may experience a silent reload. This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2. There are no known workarounds.
CSCek66377	Not all entries are seen for the Protect line card in the MIB table. There are no known workarounds.

**Table 45**      **Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsl74859	<p>If the <b>show cable modem</b> command is used after a PRE switchover, cable modems are duplicated with the same MAC address.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(00)BC3.</p> <p>There are no known workarounds.</p>
CSCek77620	<p>This issue is fixed in 12.3(21)BC4 release through CSCsj31345.</p> <p>Workaround: If you cannot ping modems, try using the <b>clear cable modem reset</b> command and retry running ping for modems.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsd14355	<p>The Simple Network Management Protocol (SNMP)-created quality of service (QoS) profile is not available after a Performance Routing Engine (PRE) switchover; the command- created QoS profile is available after switchover.</p> <p>There are no known workarounds.</p>
CSCsl79007	<p>Memory corruption at input/ output (I/O) memory occurs due to a redzone overrun, causing a PRE2 switchover.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17b) BC5.</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsl80817	<p>When making a voice call with data traffic saturation in upstream and downstream directions, the voice call packets-per-second (PPS) value is reduced to less than 49.</p> <p>The expected PPS is 49 or 50 after polling for a specific duration.</p> <p>There are no known workarounds.</p>
CSCsh19917	<p>Some parent warnings appear when static analysis is performed on the specmib source file.</p> <p>Workaround: No workaround is required. The functionality of the MIB query is not affected.</p>

**Table 45** Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)

DDTS ID Number	Description
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li data-bbox="574 422 1474 548">1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachables" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li data-bbox="574 562 1474 653">2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachables" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh41508	<p>The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.</p> <p>There are no known workarounds.</p>
CSCs189471	<p>WB modem does not change to wideband-online status after adding <b>modular-host subslot</b>.</p> <p>This problem is seen when <b>modular-host subslot</b> is configured on any modular controller and FN is configured instead of Channel Grouping Domain (CGD).</p> <p>Workaround: Configure CGD before adding <b>modular-host subslot</b>.</p>
CSCsh66150	<p>The <b>show cable modem connectivity</b> command output is corrupted under some condition.</p> <p>The following example shows a sample output.</p> <pre data-bbox="574 1234 1474 1514"> ----- show cable modem connectivity ----- Prim 1st time   Times %online   Online time           Offline time Sid  online      Online      min   avg   max   min   avg max 9    04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 11   04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00                     </pre> <p>This issue occurs after PRE switchover.</p> <p>Workaround: Clear cable modem delete.</p>
CSCs190289	<p>When the dynamic interleaver (via the upstream modulation profile) is enabled on the MC5x20H BPE line card all cable modems go offline after several hours.</p> <p>There are no known workarounds.</p>
CSCsh69870	<p>The VTMS algorithm has to be optimized due when CMs with different MIRs are mixed. The Downstream can not be fully utilize by a CM configured with a very high MIR (16-20Mbps), even when there is BW available in such Downstream.</p> <p>There are no known workarounds.</p>

**Table 45**      **Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh70679	<p>When sending a trap due to exceeding a threshold, the admission control system fails to report the correct type of event that triggered the threshold to be exceeded.</p> <p>There are no known workarounds.</p>
CSCsh72785	<p>No SNMP trap is generated on behalf of the redundant PRE state change.</p> <p>This issue may occur on the redundant PRE configuration and state change of redundant unit.</p> <p>There are no known workarounds.</p>
CSCsh95096	<p>On a Cisco uBR10012 running Cisco IOS Release 12.3(21)BC, it is possible to change default connector commands even if modems are online on that upstream connector.</p> <p>There are no known workarounds.</p>
CSCsh96105	<p>Under the following conditions, tracebacks are seen and the modem does not come online.</p> <ul style="list-style-type: none"> <li>• HCCP is configured and activated.</li> <li>• A modem changes upstream to an DOCSIS 2.0 only channel.</li> </ul> <p>Workaround: Delete the modem and let it come online again.</p>
CSCsi05236	<p>When the Ubr10k Half-Height GE linecard is connected to the SCE2000 GE link and both are configured with auto-negotiation, the link does not come up. This problem does not exist for the Full-Height GE.</p> <p>This issue occurs when an Ubr10k Half-Height GE is directly connected to the SCE GE link and auto-negotiation is turned on both links.</p> <p>Workaround: If the auto-negotiation is removed from both GE interfaces, then the link will come up.</p>
CSCsi09848	<p>Pagent cannot get a predefined IP DHCP pool so it will automatically be assigned the default. (192.168.100.x).</p> <p>This issue occurs when running HA regression cases.</p> <p>Workaround: Rerun the case.</p>
CSCsi27520	<p>The following interface RPF configuration commands are accepted on theubr10k even though they are not supported in theubr10k microcode:</p> <p><b>ip unicast source reachable-via any allow-default</b></p> <p><b>ip unicast source reachable-via rx &lt;1-199&gt;</b></p> <p><b>ip unicast source reachable-via rx &lt;1300-2699&gt;</b></p> <p>Workaround: Do not configure the unsupported commands.</p>

Table 45 Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)

DDTS ID Number	Description
CSCsi33625	<p>The code automatically changes the acceptable upstream (US) power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This setting is legal for all US channel width options.</p>
CSCsi41787	<p>The <b>show int if downstream</b> CLI shows “cable interface downstream is up” even though the interface is in shutdown state.</p> <p>There are no known workarounds.</p>
CSCsI91048	<p>The <b>show tech-support</b> and <b>show cable tech-support</b> commands do not provide information about <b>modular-cable x/y/z</b> and <b>jacket x/y</b> in privileged EXEC mode.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(21a) BC3.</p> <p>Workaround: Manually collect the following data:</p> <ul style="list-style-type: none"> <li>• Show controller jacket x/y</li> <li>• Show controller modular-cable x/y/z</li> </ul>
CSCsI96432	<p>The association between a customer premises equipment (CPE) and a cable modem (CM) is lost after an N+1 switchover even though the host route determined by the Routing Information Protocol (RIP) appears in the VPN routing/forwarding (VRF) table.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a) BC2.</p> <p>Workaround: Ping the CPE from the CMTS to update the CM/ CPE association.</p>
CSCsi48608	<p>ACL configured to the CPE is not available after line card/interface switchover.</p> <p>This issue occurs when using <b>cable {modem   host   device} access-group acl</b>.</p> <p>Workaround: Reconfigure ACL to the CPE manually after switchover.</p>
CSCsI98243	<p>Syslog messages are logged on the syslog server using one of the Gigabit Ethernet interfaces instead of the specified loopback interface.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(21a) BC3.</p> <p>Workaround: Reapply the <b>no logging source-interface Loopback0</b> and <b>logging source-interface Loopback0</b> commands.</p>

**Table 45** *Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsm08382	<p>When using the aggregate cdxIfCmtsServiceOutOctets MIB variable to obtain downstream byte counter statistics, some modems report a zero value for the downstream byte counter aggregate MIB.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3 (17b) BC4 or 12.3 (21a) BCx.</p> <p>From DOCSIS 1.1 onwards, statistics are maintained for each service flow, instead of the Service ID, in the DOCS-QOS-MIB in docsQosServiceFlowStatsTable objects. For cable modems not running in DOCSIS 1.0 mode, the objects cdxIfCmtsServiceOutOctets and cdxIfCmtsServiceOutPackets will only support primary service flow.</p> <p>There are no known workarounds.</p>
CSCsi81513	<p>HCCP status shows that everything is synced and the Protect is ready for switchover, even though nothing has been synced over and the interdb on the Protect LC is empty.</p> <p>A LC switchover after this is totally broken and modems will never register on the Protect LC</p> <p>This happens only when the Blaze FPGA image is changed for the Modena and is being reprogrammed on CMTS bootup.</p> <p>Workaround: The modems will not register on the modular interface when Blaze FPGA is being reprogrammed. As soon as the Blaze is reprogrammed, reload the CMTS as the modems are already down.</p> <p>On reload everything should work correctly.</p>
CSCsi85054	<p>When dynamic cable modem load balancing is configured between downstream A and downstream B, and downstream B's service flow admission control thresholds are significantly lower than downstream A's. It appears that load balancing still moves modems across to downstream B, even after violating the prescribed Admission control limits.</p> <p>There are no known workarounds.</p>
CSCsi87195	<p>When you configure frequency using SNMP, the range of frequencies accepted is based on the following formula.</p> $\text{min\_us\_freq} = 5000000 + (\text{channel\_width}/2)$ $\text{max\_us\_freq} = 55000000 - (\text{channel\_width}/2)$ <p>Given a frequency configured, when configuring a channel width that cannot accept the frequency configured already, there should be warning message saying that "channel width cannot be configured with the present frequency".</p> <p>This problem occurs when the frequency you are trying to configure via SNMP is not within the channel width currently configured on the CMTS router.</p> <p>There are no known workarounds.</p>
CSCsj12497	<p>When the <b>cable per-dev-acl</b> command is configured, the access-list assigned to the host is not available after a PRE switchover.</p> <p>There are no known workarounds.</p>

**Table 45** Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)

DDTS ID Number	Description
CSCsj58093	<p>CPE ping stops after the wideband (WB) switches to the narrowband (NB) mode. This problem occurs when you shut down the WB interface.</p> <p>Workaround: Execute <b>clear arp</b> or <b>clear cable modem</b> commands to clear the ARP entries and then let the cable modem on the NB to come online.</p>
CSCsj64207	<p>It seems that the total downstream rate applied to Annex A 256QAM downstreams by admission control is only 1543127 bits per second, as opposed to the real rate which is somewhere around 50Mbps.</p> <p>There are no known workarounds.</p>
CSCsj84440	<p>Adding an RF channel to a WB interface, by configuring <b>cable rf-channel</b> under wideband-cable interface, will cause the corresponding wideband modems to leave w-online state with a “Fiber node x status changed to Invalid state” message shown in CLI.</p> <p>If the RF channel is currently in a fiber node and it is also used by a WB interface, and the fiber node is in a “Valid” state. If this RF channel is added to a new WB interface that does not yet have bundle configured (or a different bundle configured), the fiber node will become “Invalid” due to mismatched bundle number. This will cause the failure of the MD-DS-SG creation and thus WB modem offline.</p> <p>Workaround: Avoid adding a RF channel to a WB interface with a different bundle configuration than the existing one.</p>
CSCsk07617	<p>The <b>show cable modem qos</b> command incorrectly shows the original ToS mask after overwrite.</p> <p>There are no known workarounds.</p>
CSCsk10852	<p>RF channel mismatch error occurs when you run the <b>show hw-module bay association wideband-channel</b> command.</p> <p>There are no known workarounds.</p>
CSCsk12224	<p>After LC switchover, modems cannot be assigned with any CM-created DOCSIS 1.0 QoS profile. The <b>cable modem qos profile</b> command works but the profile does not get assigned</p> <p>The defect is seen in all software releases.</p> <p>Workaround: Delete the modem before assigning the CM-created QoS profile using the <b>clear cable modem delete</b> command.</p>
CSCsk20304	<p>When using the <b>show cable bundle</b> command with traffic going to a CPE device behind a wideband cable modem, the data going to the CPE is not seen on the bundle interface that it is using. This data will appear on the input GE port and the wideband interface.</p> <p>There are no known workarounds.</p>
CSCsk28938	<p>On a uBR10k running 12.3(17a)BC and up (and older code, as well), the <b>cable downstream rate-limit</b> command has no affect on DS traffic.</p> <p>There are no known workarounds.</p>

**Table 45** *Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsk39347	<p>During the Online Insertion and Removal (OIR) process in an HA WORKING line card, all modems failover to the PROTECT mode, resulting in a loss of the PCMM gates or test PacketCable. However, the dynamic service flows and PCMM voice calls function normally.</p> <p>There are no known workarounds.</p>
CSCsk41698	<p>In the following scenario, if a customer mistakenly configures LC 5/0 as PROTECT, plus the <b>no mem sub x/y revertive</b> command and then corrects the problem by configuring LC 5/1 as PROTECT, the <b>no mem sub x/y revertive</b> command is not reflected in the <b>show hccp detail</b> output.</p> <p>Workaround: Reconfigure the <b>no mem sub x/y revertive</b> command.</p>
CSCsk53180	<p>The output of <b>show controllers cx/y/z tech-support</b> contains passwords in the running-configuration. These passwords should be removed, as these tech-support reports are routinely sent to TAC via non-secure email.</p> <p>There are no known workarounds.</p>
CSCsk65431	<p>Changing IP add on the int bundle X.1 subinterface results in an Integrated Up-converter flap for all interfaces associated with that bundle.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17)BC or higher that has a bundle interface configured.</p> <p>There are no known workarounds.</p>
CSCsk68026	<p>Bus error exception crash on PRE of uBr10k.</p> <p>This issue occurs on an uBr10k with IOS 12.3(21a)BC2, seen on PRE1 as well as PRE2.</p> <p>There are no known workarounds.</p>
CSCsk72430	<p>Increasing docsis frag header discard counters are seen in 12.3(21a)BC3 when running US at high utilization rate. This problems affect multiple CMs.</p> <p>Workaround: Disable docsis frag.</p>
CSCsk85933	<p>A uBR10k running 12.3(17b)BC3 may report Cable Modems stuck in init(rc) state on certain Upstream Interfaces. Very high number of Input queue drops are also observed under the corresponding Downstream interfaces.</p> <p>This problem has only been observed on uBR10K with MC5x20H-D card.</p> <p>Workaround: Resetting the line card will bring all the Cable Modems back to online.</p>
CSCsl06036	<p>Maxcpe functionality is broken with w-online modems. The functionality is working with the same modem in the same image when it registered in the online state.</p> <p>There are no known workarounds.</p>

Table 45 Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)

DDTS ID Number	Description
CSCs110231	<p>A downstream service flow with an associated classifier will have the classifier “match count” initialized to zero if there is a PRE switchover or a reload of the pxf.</p> <p>This issue occurs on a service flow with a classifier and PRE switchover or pxf reload.</p> <p>There are no known workarounds.</p>
CSCs126209	<p>uBR10000 with PRE2 reports inconsistent (much lower) input byte rate and packet rate than directly attached device over GE interface.</p> <p>The issue appears to be cosmetic affecting traffic counters only. This is observable only when GE interface has 802.1q tagged subinterfaces configured.</p> <p>There are no known workarounds.</p>
CSCs137665	<p>Since the service flow is not in active state, “cable service flow activity-timeout 1800” will not help. Another timer which is “Admitted QoS timer” should have kicked in and cleaned it. Since that did not happen it is still an issue.</p> <p>There is no equivalent command to clean out service flows in admitted state.</p> <p>Customer has a non-packet VOIP service, and currently have the activity-timeout set to 1800 seconds (implemented about 4 months ago) this value is what is being placed as the Active QoS timeout.</p> <p>Workaround: Try clearing the Cable Modem using the command <b>clear cable modem</b>. If there are many flows, you could also try to script it.</p>
CSCs142554	<p>All CMs became offline with no alert or log message. When <b>clear cable modem all delete</b> command was executed, no CM was ranging. When checked, upconverter signal was ok and ucd counter also normal.</p> <p>This issue is observed in routers with the Cisco MC520H linecard.</p> <p>Workaround: Use <b>cable downstream rf-shutdown</b> and <b>no cable downstream rf-shutdown</b> commands.</p>
CSCs142777	<p>Traceback observed in <code>cmts_cgd_get_active_primary</code> on the secondary PRE when image is upgraded resulting in a SPA FPGA upgrade.</p> <p>Modular cable interfaces are configured with the 12.3(23)BC and associated with a “Channel Grouping Domain” using the <b>downstream modular-cable interface</b> command.</p> <p>There are no known workarounds.</p>
CSCs143172	<p>Traceback observed during cable linecard switchover on the linecard becoming active.</p> <p>Modular cable interfaces are configured and associated with a “Channel Grouping Domain” using the <b>downstream Modular-Cable</b> interface command</p> <p>There are no known workarounds.</p>

**Table 45**      **Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)**

DDTS ID Number	Description
CSCsl43380	<p>After multiple interfaces on different 520 linecards switchover and then revert, UBR10K-6-CM-INCONSISTENCY messages may be seen for wideband modems, and those modems will flap.</p> <p>This problem affects 12.3BC(23) and is seen with the following conditions.</p> <ol style="list-style-type: none"> <li>1. HCCP is configured with interface commands.</li> <li>2. Interfaces on multiple linecards switchover.</li> <li>3. One or more interfaces that switchover are on a linecard that is the modular-host for a SPA.</li> </ol> <p>Workaround: This problem will not occur if HCCP is configured with global commands, which force all interfaces on a linecard to switchover.</p>
CSCsl45841	<p>Call drops and PSQM failures observed when making bulk packetcable calls.</p> <p>There are no known workarounds.</p>
CSCsl49206	<p>If the associated HA <b>ip host</b> commands are removed followed by PRE switchovers from PREA to PREB and then from PREB to PREA. After re-configuring the Global HA commands, all modems disappear, re-range and then come back online.</p> <p>There are no known workarounds.</p>
CSCsl50048	<p>Modems cannot register on modular-cable downstreams when they use config files that have downstream llq (max downstream latency) set, but do not have min and max DS rate configured.</p> <p>These modems are stuck in reject(c) state</p> <p>Workaround: Add min and max DS rate in the downstream service flow encoding in the configuration file.</p>
CSCsl57014	<p>An unexpected crash occurs when executing a <b>show ip interface brief</b> soon after load and bootup.</p> <p>There are no known workarounds.</p>
CSCsl57849	<p>Voice subs experience one way audio</p> <p>Workaround: Issue the <b>hw-module slot x stop/start</b> command.</p>
CSCsl57861	<p>OIR removal of the DOCSIS downstream SPA will cause modems using the modular downstreams of the other SPA to go offline.</p> <p>The PXF queues used for MAP traffic are stuck and have continuous tail drops. The MAP queue id for a SPA can be found in <b>show pxf cpu queue wb-spa</b> command.</p> <p>Heavy load (data and DOCSIS MAC management traffic including MAPs) on the SPA jacket card increase the chances of running into this issue</p> <p>Workaround: Stop all traffic to the SPA before the OIR removal by shutting down all the Modular-Cable and Wideband interface associated with the SPA.</p> <p>If the interfaces are not shutdown then reset Saratoga Jacket card if these symptoms occur after the SPA OIR.</p>

**Table 45** Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)

DDTS ID Number	Description
CSCs171939	<p>On a DOCSIS1.0 modem, multiple customer premises equipments (CPE) get IP addresses when the <b>max-cpe</b> value is set to 1.</p> <p>There are no known workarounds.</p>
CSCs172140	<p>Few modems, with similar configurations, were stuck in the <b>init(io)</b> state and could not proceed further.</p> <p>Workaround: Execute <b>clear cable modem [mac-address] delete</b> command.</p>
CSCs173846	<p>A Modular Cable interface may result in an unexpected behavior after a quick <b>shutdown</b> and <b>no shutdown</b>.</p> <p>Workaround: After shutting down a Modular Cable interface, wait for at least five seconds before proceeding with any further configuration.</p>
CSCs173926	<p>On a wideband SPA (Shared Port Adapter), when one SFP module is disconnected the other module does not connect as expected.</p> <p>There are no known workarounds.</p>
CSCs174050	<p>Unable to ping the w-online modem when the committed information rate (CIR) is very high.</p> <p>Workaround: Ensure that the CIR of WCM service flows is less than the CIR of the WB interface.</p>
CSCsk31357	<p>PCMM gates will not be synced to the standby RP. Hence, if there is a PRE switchover, the newly active RP will not have the PCMM gate information.</p> <p>This issue occurs when running config only has “packetcable multimedia” enabled but not “packetcable”.</p> <p>Workaround: Enable “packetcable” in running configuration.</p>
CSCsj12597	<p>As part of OSSSI requirement, dot3StatsCarrierSenseErrors need to incremented when the cable is removed from FE Interface. However, this is not happening.</p> <p>There are no known workarounds.</p>

**Table 45** Open Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)

DDTS ID Number	Description
CSCsk60014	<p>Symptom: No downstream throughput for PC calls on eMTA accompanied by a warning after a PRE failover. The problem occurs because the standby PRE fails to start its WBCMTS periodic timer after the failover. When the problem occurs wideband capable modems fail to come online in wideband mode and register as narrowband modems instead.</p> <p>Condition: The problem occurs if the failover happens before the Wideband SPA has reached its operational state. This could happen if the card was not inserted prior to the failover. This could also happen if the failover occurred concurrently with downloading the operational firmware. For example, it could happen if the active and standby PREs boot simultaneously and the active PRE is in the process of bringing up the WB SPA when a PRE failover occurs.</p> <p>Workaround: Reload the router.</p>
CSCsj14502	<p>In certain cases, CMTS does not send intercept packets out in case of cTapStreamIpInterface is set to -1, while other parameters are set correctly in cTapStreamIpTable and snmpwalk show the cTapStreamIpStatus is active.</p> <p>The issue occurs when configuring a cTapStreamIp entry as follows:</p> <pre> cTapStreamIpInterface = -1 cTapStreamIpDestinationAddress = Addr1 cTapStreamIpDestinationLength = 32 cTapStreamIpSourceAddress = Addr2 cTapStreamIpSourceLength = 32 </pre> <p>and Addr1 is directly connected to a cable interface, Addr2 is routed through another interface and the net mask of outgoing interface for destination Addr2 is greater than the one of Addr1.</p> <p>Workaround: Perform one of the following:</p> <p>(1) Directly set the tapping interface's IfIndex, letting cTapStreamIpInterface != -1 and != 0</p> <p>(2) or, Either set cTapStreamIpSourceAddress or cTapStreamIpDestinationAddress to zero, to avoid conflict.</p>

## Resolved Caveats for Release 12.3(21a)BC5

Table 46 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC5.

**Table 46 Resolved Caveats for Cisco IOS Release 12.3(21a)BC5**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsk52258	<p>An UBR10000-3-INVALID_INVOKE_FROM_ISR error message, along with a traceback, occurs.</p> <p>In a WB setup, a corner case scenario causes the CM to send a B-INIT-RNG request on a non-broadcast slot and thus causing the invalid invoke from ISR error.</p> <p>There are no known workarounds.</p>
CSCs132472	<p>Cable Modems receive one-third to one-fourth of the bandwidth on few downstreams. However, not all downstreams on the Cisco uBR10-MC5X20U linecard are affected, except some upstreams.</p> <p>This issue occurs on uBR10k running Cisco IOS Release 12.3(21a) BC1 with 520u cards.</p> <p>Workaround: Reload the parallel express forwarding (PXF).</p>
CSCs134893	<p>ARP table entries are incorrect for a CPE. This can result in CPE traffic being sent to the wrong modem.</p> <p>The ARP table issue occurs for CPEs that move from one modem to another or when one CPE goes away and the IP address is allocated to another CPE by the DHCP server.</p> <p>There are no known workarounds.</p>
CSCs154498	<p>An UBR10000-3-INVALID_INVOKE_FROM_ISR error message, along with a traceback, occurs.</p> <p>In a WB setup, a corner case scenario causes the CM to send a B-INIT-RNG request on a non-broadcast slot and thus causing the invalid invoke from ISR error.</p> <p>There are no known workarounds.</p>
CSCs119255	<p>Pre-allocated queues do not get pre-allocated for downstream interfaces above 40. This could potentially create an issue for newly created interfaces in the event that the router is undergoing BE queue aggregation. The symptom would be that if the router was undergoing BE queue aggregation and new interfaces were added to the configuration, modems could fail to come online on the newly created interfaces.</p> <p>The condition exists when there are more than 40 downstream interfaces. Prior to this release the maximum number of downstream interfaces that could be provisioned on the uBR10k was 40. Support for Modular Cable and Wideband Cable increases this maximum to greater than 40. The infrastructure fails to provide pre-allocated queues for newly created downstream interfaces.</p> <p>Workaround: The workaround would be to provision new interfaces, when the new downstream interfaces would increase the total number of downstream interfaces to greater than 40, and then reload the router.</p>
CSCsk25070	<p>Executing a <b>show packetcable gate summary</b> after oir a cable line card will cause a system crash.</p> <p>This only occurs at the time hccp is deconfured at the packetcable call are on going in that cable line card.</p> <p>Workaround: Stop calls before using OIR on the card.</p>

**Table 46 Resolved Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)**

DDTS ID Number	Description
CSCsl32567	<p>When executing <b>show aaa attribute protocol radius</b> command, the router running Cisco IOS may crash or display junk characters.</p> <p>There are no known workarounds.</p>
CSCsk41966	<p>On a nubr10k running 12.3(21a)BC2, the interface mac-scheduler reports higher number of active UGS flows than active calls reported by "show cable calls" for that interface. It also holds the UGS flow BW and do not release. UGS flows are NOT stuck though.</p> <p>The following is an example:</p> <pre>show cable calls reports 2 active UGS calls while mac-scheduler reports 17.</pre> <pre>Router#sh cable modem calls   i 8/1/2/U0 0011.e3ef.6e3d 10.66.50.91 C8/1/2/U0 4029 V - 0011.e3ec.cee2 10.66.52.184 C8/1/2/U0 2143 V</pre> <pre>Router#sh int c8/1/2 mac-scheduler 0 &lt;snip&gt;</pre> <pre>ched Table Adm-State: Grants 17, Reqpolls 0, Util 19% UGS : 17 SIDs, Reservation-level in bps 1543600</pre> <p>Router#</p> <p>This issue is only observed when DS load balancing is enable and only on the USs, which are a part of the LB group.</p> <p>There are no known workarounds.</p>
CSCsk63745	<p>Reduced downstream throughput occurs over time on uBR10k routers with &gt;40000 modems.</p> <p>BE queue aggregation must be taking place for this problem to occur.</p> <p>There are no known workarounds.</p>
CSCsk53235	<p>If config ip access-group in on a cable bundle interface, then delete this interface using command <b>no interface bundle n</b>. Then recreate the bundle interface, configure ip access-group in on the interface and the traceback appears.</p> <p>This issue is seen in a uBR10k running 12.3(23)BC.</p> <p>There are no known workarounds.</p>
CSCsl09172	<p>The <b>show inventory</b> command does not provide the secondary Performance Routing Engine (PRE) serial number.</p> <p>Workaround: Enable the <b>secondary console enable</b> hidden command before logging into the secondary console and then run the command to obtain secondary PRE serial number.</p>

**Table 46 Resolved Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)**

DDTS ID Number	Description
CSCsl69376	<p>After two or more of PRE switchovers by the admin for IOS upgrade, all CMs connected to the systems will encounter download speeds less than 1Mbps.</p> <p>This issue occurs whenever two or more PRE switchovers are executed. This error occurred in 12.3(17b)BC3 and BC5. When tested in 12.3(13a)BC3 and 12.3(21)BC, there was no problem.</p> <p>Workaround: Performing a CM disconnect and reconnect solves this problem.</p>
CSCsk74917	<p>CMTS crashes.</p> <p>This is a rare situation and only occurs when the current or next element in cm_list_hdr has been deleted by another process during process suspend, and the function does not enough check to ensure the list sanity.</p> <p>There are no known workarounds.</p>
CSCsk28584	<p>Unable to remove the remote query community string.</p> <p>This issue occurs when un-configuring an invalid remote query community string.</p> <p>Workaround: Wait for some time after un-configuration and the community string will disappear.</p>
CSCsl40446	<p>CMTS uses the wrong rf-switch snmp community string during a LC switchover from W to P. As a consequence, once the modems failover to the PROTECT card, they fall offline and never come online. This issue is seen after configuring a rf-switch snmp community string, followed by PRE failovers from PREA to PREB and then back from PREB to PREA and then removing the configured rf-switch snmp community string.</p> <p>There are no known workarounds.</p>

**Table 46 Resolved Caveats for Cisco IOS Release 12.3(21a)BC5 (continued)**

DDTS ID Number	Description
CSCsk70446	<p>Traceback observed while using long URLs to configure a device using the Cisco IOS HTTP web parser.</p> <p>This issue occurs while trying to configure commands that have a single keyword or parameter greater than N characters in length, where N is:</p> <ul style="list-style-type: none"> <li>• 50 for Cisco IOS Release 12.0 and above</li> <li>• 128 for Cisco IOS Release 12.2 and above</li> <li>• 256 for Cisco IOS Release 12.2(25) and above</li> </ul> <p>Workaround: Avoid using the Cisco IOS HTTP web parser for commands with long keywords or arguments.</p>
CSCsk40979	<p>On a Cisco uBR10012 router running 12.3(21a)BC2, the interface mac-scheduler reports higher number of active UGS flows then active calls reported by "show cable calls" for that interface. It also holds the UGS flow BW and do not release. UGS flows are NOT stuck though.</p> <p>The following is an example:</p> <pre>show cable calls reports 2 active UGS calls while mac-scheduler reports 17.</pre> <pre>Router#sh cable modem calls   i 8/1/2/U0 0011.e3ef.6e3d 10.66.50.91 C8/1/2/U0 4029 V - 0011.e3ec.cee2 10.66.52.184 C8/1/2/U0 2143 V</pre> <pre>Router#sh int c8/1/2 mac-scheduler 0 &lt;snip&gt;</pre> <pre>ched Table Adm-State: Grants 17, Reqpolls 0, Util 19% UGS : 17 SIDs, Reservation-level in bps 1543600</pre> <pre>Router#</pre> <p>This issue is only observed when DS load balancing is enable and only on the USs, which are a part of the LB group.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(23)BC

Table 47 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(23)BC.

**Table 47**      **Open Caveats for Cisco IOS Release 12.3(23)BC**

<b>DDTS ID Number</b>	<b>Description</b>
CSCek41611	<p>Cisco uBR10-MC5X20U cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>
CSCsd14355	<p>The Simple Network Management Protocol (SNMP)-created quality of service (QoS) profile is not available after a Performance Routing Engine (PRE) switchover; the command- created QoS profile is available after switchover.</p> <p>There are no known workarounds.</p>
CSCs119255	<p>Pre-allocated queues do not get pre-allocated for downstream interfaces above 40. This could potentially create an issue for newly created interfaces in the event that the router is undergoing BE queue aggregation. The symptom would be that if the router was undergoing BE queue aggregation and new interfaces were added to the configuration, modems could fail to come online on the newly created interfaces.</p> <p>The condition exists when there are more than 40 downstream interfaces. Prior to this release the maximum number of downstream interfaces that could be provisioned on the uBR10k was 40. Support for Modular Cable and Wideband Cable increases this maximum to greater than 40. The infrastructure fails to provide pre-allocated queues for newly created downstream interfaces.</p> <p>Workaround: The workaround would be to provision new interfaces, when the new downstream interfaces would increase the total number of downstream interfaces to greater than 40, and then reload the router.</p>
CSCsh69870	<p>The VTMS algorithm has to be optimized due when CMs with different MIRs are mixed. The Downstream can not be fully utilize by a CM configured with a very high MIR (16-20Mbps), even when there is BW available in such Downstream.</p> <p>There are no known workarounds.</p>
CSCsi05236	<p>When the Ubr10k Half-Height GE linecard is connected to the SCE2000 GE link and both are configured with auto-negotiation, the link does not come up. This problem does not exist for the Full-Height GE.</p> <p>This issue occurs when an Ubr10k Half-Height GE is directly connected to the SCE GE link and auto-negotiation is turned on both links.</p> <p>Workaround: If the auto-negotiation is removed from both GE interfaces, then the link will come up.</p>

**Table 47**      **Open Caveats for Cisco IOS Release 12.3(23)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsj84440	<p>Adding an RF channel to a WB interface, by configuring <b>cable rf-channel</b> under wideband-cable interface, will cause the corresponding wideband modems to leave w-online state with a “Fiber node x status changed to Invalid state” message shown in CLI.</p> <p>If the RF channel is currently in a fiber node and it is also used by a WB interface, and the fiber node is in a “Valid” state. If this RF channel is added to a new WB interface that does not yet have bundle configured (or a different bundle configured), the fiber node will become “Invalid” due to mismatched bundle number. This will cause the failure of the MD-DS-SG creation and thus WB modem offline.</p> <p>Workaround: Avoid adding a RF channel to a WB interface with a different bundle configuration than the existing one.</p>
CSCsj98444	<p>Although the <b>snmpgetnext</b> command succeeds, the <b>snmpget</b> command returns a “(noSuchName)” error.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17b)BC6 with the Performance Routing Engine 1 (PRE1) and UBR10-MC5X20U-D- CM.</p> <p>There are no known workarounds.</p>
CSCsk12224	<p>After LC switchover, modems cannot be assigned with any CM-created DOCSIS 1.0 QoS profile. The <b>cable modem qos profile</b> command works but the profile does not get assigned</p> <p>The defect is seen in all software releases.</p> <p>Workaround: Delete the modem before assigning the CM-created QoS profile using the <b>clear cable modem delete</b> command.</p>
CSCsk20304	<p>When using the <b>show cable bundle</b> command with traffic going to a CPE device behind a wideband cable modem, the data going to the CPE is not seen on the bundle interface that it is using. This data will appear on the input GE port and the wideband interface.</p> <p>There are no known workarounds.</p>

Table 47 Open Caveats for Cisco IOS Release 12.3(23)BC (continued)

DDTS ID Number	Description
CSCsk40979	<p>On a Cisco uBR10012 router running 12.3(21a)BC2, the interface mac-scheduler reports higher number of active UGS flows than active calls reported by "show cable calls" for that interface. It also holds the UGS flow BW and do not release. UGS flows are NOT stuck though.</p> <p>The following is an example:</p> <pre>show cable calls reports 2 active UGS calls while mac-scheduler reports 17.</pre> <pre>Router#sh cable modem calls   i 8/1/2/U0 0011.e3ef.6e3d 10.66.50.91 C8/1/2/U0 4029 V - 0011.e3ec.cee2 10.66.52.184 C8/1/2/U0 2143 V</pre> <pre>Router#sh int c8/1/2 mac-scheduler 0 &lt;snip&gt;</pre> <pre>ched Table Adm-State: Grants 17, Reqpolls 0, Util 19% UGS : 17 SIDs, Reservation-level in bps 1543600</pre> <p>Router#</p> <p>This issue is only observed when DS load balancing is enable and only on the USs, which are a part of the LB group.</p> <p>There are no known workarounds.</p>
CSCsk41966	<p>A UBR that uses 127.x.x.x prefixes for internal management will include these prefixes in its LDP/TDP address and label mapping messages. Peering routers that have a fix for CSCdx08804 or CSCdx88897 will display error messages like:</p> <pre>%TAGCON-3-TDPID: peer 192.168.254.253:0, TDP Id/Addr mapping problem (rcvd invalid address in TDP address PIE, ignored) %TAGCON-3-TDPID: peer 192.168.254.253:0, TDP Id/Addr mapping problem (rcvd TDP address PIE, bind failed) %TIB-3-REMOTETAG: 127.3.0.0/255.255.0.0, peer 192.168.254.253:0; tag 1; add tag failure</pre> <p>The error messages are harmless. They indicate that the peer has advertised invalid host/network IP addresses, and the receiving router has accordingly ignored the associated advertisements.</p> <p>There are no known workarounds.</p>
CSCsk53235	<p>If config ip access-group in on a cable bundle interface, then delete this interface using command <b>no interface bundle n</b>. Then recreate the bundle interface, configure ip access-group in on the interface and the traceback appears.</p> <p>This issue is seen in a uBR10k running 12.3(23)BC.</p> <p>There are no known workarounds.</p>
CSCsk63745	<p>Reduced downstream throughput occurs over time on uBR10k routers with &gt;40000 modems.</p> <p>BE queue aggregation must be taking place for this problem to occur.</p> <p>There are no known workarounds.</p>

**Table 47** *Open Caveats for Cisco IOS Release 12.3(23)BC (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsk68026	<p>Bus error exception crash on PRE of ubr10k.</p> <p>This issue occurs on an ubr10k with IOS 12.3(21a)BC2, seen on PRE1 as well as PRE2.</p> <p>There are no known workarounds.</p>
CSCsk72430	<p>Increasing docsis frag header discard counters are seen in 12.3(21a)BC3 when running US at high utilization rate. This problems affect multiple CMs.</p> <p>Workaround: Disable docsis frag.</p>
CSCsk85933	<p>A uBR10k running 12.3(17b)BC3 may report Cable Modems stuck in init(rc) state on certain Upstream Interfaces. Very high number of Input queue drops are also observed under the corresponding Downstream interfaces.</p> <p>This problem has only been observed on uBR10K with MC5x20H-D card.</p> <p>Workaround: Resetting the line card will bring all the Cable Modems back to online.</p>
CSCsk86886	<p>A Cisco router running IOS version 123(17b)BC8 may reload unexpectedly.</p> <p>There are no known workarounds.</p>
CSCsl06036	<p>Maxcpe functionality is broken with w-online modems. The functionality is working with the same modem in the same image when it registered in the online state.</p> <p>There are no known workarounds.</p>
CSCsl07388	<p>Cisco uBR10-MC5X20U linecard crashes with Illegal access to a low address errors and a crashfile written.</p> <p>Crashes are experienced on Cisco uBR10-MC5X20U linecards in ubr10000 running 12.3(21a)BC2.</p> <p>There are no known workarounds.</p>
CSCsl10231	<p>A downstream service flow with an associated classifier will have the classifier “match count” initialized to zero if there is a PRE switchover or a reload of the pxf.</p> <p>This issue occurs on a service flow with a classifier and PRE switchover or pxf reload.</p> <p>There are no known workarounds.</p>

Table 47 Open Caveats for Cisco IOS Release 12.3(23)BC (continued)

DDTS ID Number	Description
CSCs119255	<p>Pre-allocated queues do not get pre-allocated for downstream interfaces above 40. This could potentially create an issue for newly created interfaces in the event that the router is undergoing BE queue aggregation. The symptom would be that if the router was undergoing BE queue aggregation and new interfaces were added to the configuration, modems could fail to come online on the newly created interfaces.</p> <p>The condition exists when there are more than 40 downstream interfaces. Prior to this release the maximum number of downstream interfaces that could be provisioned on the uBR10k was 40. Support for Modular Cable and Wideband Cable increases this maximum to greater than 40. The infrastructure fails to provide pre-allocated queues for newly created downstream interfaces.</p> <p>Workaround: Provision new interfaces. When the new downstream interfaces would increase the total number of downstream interfaces to greater than 40, and then reload the router.</p>
CSCs126209	<p>uBR10000 with PRE2 reports inconsistent (much lower) input byte rate and packet rate than directly attached device over GE interface.</p> <p>The issue appears to be cosmetic affecting traffic counters only. This is observable only when GE interface has 802.1q tagged subinterfaces configured.</p> <p>There are no known workarounds.</p>
CSCs137665	<p>Since the service flow is not in active state, “cable service flow activity-timeout 1800” will not help. Another timer which is “Admitted QoS timer” should have kicked in and cleaned it. Since that did not happen it is still an issue.</p> <p>There is no equivalent command to clean out service flows in admitted state.</p> <p>Customer has a non-packet VOIP service, and currently have the activity-timeout set to 1800 seconds (implemented about 4 months ago) this value is what is being placed as the Active QoS timeout.</p> <p>Workaround: Try clearing the Cable Modem using the command <b>clear cable modem</b>. If there are many flows, you could also try to script it.</p>
CSCs138692	<p>If an uBR10K run on 12.3(13)BC6 is upgrade to 12.3(21)BC3, then Ifindex is change.</p> <p>There are no known workarounds.</p>
CSCs140446	<p>The CMTS uses the wrong rf-switch snmp community string during a LC switchover from W to P. As a consequence, once the modems failover to the PROTECT card, they fall offline and never come online. This issue is seen after configuring a rf-switch snmp community string, followed by PRE failovers from PREA to PREB and then back from PREB to PREA and then removing the configured rf-switch snmp community string.</p> <p>There are no known workarounds.</p>
CSCs142554	<p>All CMs became offline with no alert or log message. When <b>clear cable modem all delete</b> command was executed, no CM was ranging. When checked, upconverter signal was ok and ucd counter also normal.</p> <p>This issue is observed in routers with the Cisco MC520H linecard.</p> <p>Workaround: Use <b>cable downstream rf-shutdown</b> and <b>no cable downstream rf-shutdown</b> commands.</p>

**Table 47** *Open Caveats for Cisco IOS Release 12.3(23)BC (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsl42777	<p>Traceback observed in <code>cmts_cgd_get_active_primary</code> on the secondary PRE when image is upgraded resulting in a SPA FPGA upgrade.</p> <p>Modular cable interfaces are configured with the 12.3(23)BC and associated with a “Channel Grouping Domain” using the <b>downstream modular-cable interface</b> command.</p> <p>There are no known workarounds.</p>
CSCsl43172	<p>Traceback observed during cable linecard switchover on the linecard becoming active.</p> <p>Modular cable interfaces are configured and associated with a “Channel Grouping Domain” using the <b>downstream Modular-Cable</b> interface command</p> <p>There are no known workarounds.</p>
CSCsl43380	<p>After multiple interfaces on different 520 linecards switchover and then revert, UBR10K-6-CM-INCONSISTENCY messages may be seen for wideband modems, and those modems will flap.</p> <p>This problem affects 12.3BC(23) and is seen with the following conditions.</p> <ol style="list-style-type: none"> <li>1. HCCP is configured with interface commands.</li> <li>2. Interfaces on multiple linecards switchover.</li> <li>3. One or more interfaces that switchover are on a linecard that is the modular-host for a SPA.</li> </ol> <p>Workaround: This problem will not occur if HCCP is configured with global commands, which force all interfaces on a linecard to switchover.</p>
CSCsl45306	<p>When an SNMP Community string is configured for RF switch under the line card redundancy configuration mode, the same string gets automatically duplicated in the global snmp configuration. As a result the RF switch community string can be used by other NMS devices until the global CLI entry is manually associated with the right ACL.</p> <p>With the current behavior, it does not make any sense to have the community string configuration option under the line card redundancy section. The desired behavior is, the community string entered under the redundancy configuration mode must not be duped to global snmp configuration and the string must be exclusively available for just the RF switches.</p> <p>There are no known workarounds.</p>
CSCsl45841	<p>Call drops and PSQM failures observed when making bulk packetcable calls.</p> <p>There are no known workarounds.</p>

**Table 47** Open Caveats for Cisco IOS Release 12.3(23)BC (continued)

DDTS ID Number	Description
CSCs146630	<p>Broadband processing Engine (BPE) linecards such as 28U, 5x20 S/U/H can overwrite some mod profile parameters and be viewed with the <code>sh cab modu c/x/y/z up n</code> command. One parameter that is still being overwritten, but not displayed is the preamble on the initial maintenance and station maintenance bursts when equalization-coefficient is enabled.</p> <p>When enabling equalization-coefficient (also known as PRE-EQ), the preamble length will increase for the initial maintenance and station maintenance bursts. This is not displayed in any current show commands and can lead to incorrect calculations.</p> <p>Workaround: Possibly use <b>debug cab ucd</b> commands.</p>
CSCs149206	<p>If the associated HA <b>ip host</b> commands are removed followed by PRE switchovers from PREA to PREB and then from PREB to PREA. After re-configuring the Global HA commands, all modems disappear, re-range and then come back online.</p> <p>There are no known workarounds.</p>
CSCs150048	<p>Modems cannot register on modular-cable downstreams when they use config files that have downstream llq (max downstream latency) set, but do not have min and max DS rate configured.</p> <p>These modems are stuck in reject(c) state</p> <p>Workaround: Add min and max DS rate in the downstream service flow encoding in the configuration file.</p>
CSCs154498	<p>IPC timeout error messages and tracebacks are experienced on cable linecards after issuing <b>ip telnet source-interface loopback</b> and <b>if-console</b> commands on the CMTS.</p> <p>This issue has been seen on a UBR10012 platform running IOS 12.3(17b)BC6.</p> <p>Workaround: Reset the linecards generating the errors using <b>hw-module reset</b> or rebooting the CMTS resolves the issue.</p>
CSCs155541	<p>SNMPwalk of docsIfCmtsCmStatusValue does not show results for all the available modems. The deviation can be identified by comparing the results from the command line interface with those from the SNMPwalk.</p> <p>This is observed under normal operating conditions.</p> <p>There are no known workarounds.</p>
CSCs157014	<p>An unexpected crash occurs when executing a <b>show ip interface brief</b> soon after load and bootup.</p> <p>There are no known workarounds.</p>
CSCs157849	<p>Voice subs experience one way audio</p> <p>Workaround: Issue the <b>hw-module slot x stop/start</b> command.</p>

**Table 47** Open Caveats for Cisco IOS Release 12.3(23)BC (continued)

DDTS ID Number	Description
CSCsl57861	<p>OIR removal of the DOCSIS downstream SPA will cause modems using the modular downstreams of the other SPA to go offline.</p> <p>The PXF queues used for MAP traffic are stuck and have continuous tail drops. The MAP queue id for a SPA can be found in <b>show pxf cpu queue wb-spa</b> command.</p> <p>Heavy load (data and DOCSIS MAC management traffic including MAPs) on the SPA jacket card increase the chances of running into this issue</p> <p>Workaround: Stop all traffic to the SPA before the OIR removal by shutting down all the Modular-Cable and Wideband interface associated with the SPA.</p> <p>If the interfaces are not shutdown then reset Saratoga Jacket card if these symptoms occur after the SPA OIR.</p>
CSCsl60652	<p>Voice calls are dropped during when there is a cable linecard switchover.</p> <p>This issue occurs when the channel width configured on the upstream used by the voice modems is 3.2 MHz</p> <p>Workaround: Use channel width of 1.6 MHz to avoid voice dropouts after a switchover.</p>

## Resolved Caveats for Release 12.3(23)BC

Table 52 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(23)BC.

**Table 48** Resolved Caveats for Cisco IOS Release 12.3(23)BC

DDTS ID Number	Description
CSCek66377	<p>Not all entries are seen for the Protect line card in the MIB table.</p> <p>There are no known workarounds.</p>
CSCek77620	<p>This issue is fixed in 12.3(21)BC4 release through CSCsj31345.</p> <p>Workaround: If you cannot ping modems, try using the <b>clear cable modem reset</b> command and retry running ping for modems.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>

**Table 48 Resolved Caveats for Cisco IOS Release 12.3(23)BC (continued)**

DDTS ID Number	Description
CSCsd65958	<p>Packets per second is far greater than bytes per second on some of the linecard interfaces, which is not possible.</p> <p>This issue occurs when the layer 2 traffic contains broadcast traffic.</p> <p>There are no know workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsh04686	<p>With X25 over TCP (XOT) enabled on a router or catalyst switch, malformed traffic sent to TCP port 1998 will cause the device to reload. This was first observed in IOS 12.2(31)SB2.</p> <p>Workaround: Use IPSEC or other tunneling mechanisms to protect XOT traffic. Also, apply ACLs on affected devices so that traffic is only accepted from trusted tunnel endpoints.</p>
CSCsh19917	<p>Some parent warnings appear when static analysis is performed on the specmib source file.</p> <p>Workaround: No workaround is required. The functionality of the MIB query is not affected.</p>
CSCsh29217	<p>Cisco 10000, uBR10012 and uBR7200 series devices use a User Datagram Protocol (UDP) based Inter-Process Communication (IPC) channel that is externally reachable. An attacker could exploit this vulnerability to cause a denial of service (DoS) condition on affected devices. No other platforms are affected.</p> <p>Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc</a></p>
CSCsl34893	<p>ARP table entries are incorrect for a CPE. This can result in CPE traffic being sent to the wrong modem.</p> <p>The ARP table issue occurs for CPEs that move from one modem to another or when one CPE goes away and the IP address is allocated to another CPE by the DHCP server.</p> <p>There are no known workarounds.</p>

**Table 48 Resolved Caveats for Cisco IOS Release 12.3(23)BC (continued)**

DDTS ID Number	Description
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachables" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachables" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh41508	<p>The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.</p> <p>There are no known workarounds.</p>
CSCsh66150	<p>The <b>show cable modem connectivity</b> command output is corrupted under some condition.</p> <p>The following example shows a sample output.</p> <pre> ----- show cable modem connectivity ----- Prim 1st time   Times %online   Online time           Offline time Sid  online      Online      min   avg   max   min   avg max 9    04:45:02    1    100.00 00:00 49710d6h49710d6h00:00 00:00 00:00 11   04:45:02    1    100.00 00:00 49710d6h49710d6h00:00 00:00 00:00 </pre> <p>This issue occurs after PRE switchover.</p> <p>Workaround: Clear cable modem delete.</p>
CSCsh70679	<p>When sending a trap due to exceeding a threshold, the admission control system fails to report the correct type of event that triggered the threshold to be exceeded.</p> <p>There are no known workarounds.</p>
CSCsh72785	<p>No SNMP trap is generated on behalf of the redundant PRE state change.</p> <p>This issue may occur on the redundant PRE configuration and state change of redundant unit.</p> <p>There are no known workarounds.</p>
CSCsh95096	<p>On a Cisco uBR10012 running 12.3(21)BC, it is possible to change default connector commands even if modems are online on that upstream connector.</p> <p>There are no known workarounds.</p>

**Table 48 Resolved Caveats for Cisco IOS Release 12.3(23)BC (continued)**

DDTS ID Number	Description
CSCsh96105	<p>Under the following conditions, tracebacks are seen and the modem does not come online.</p> <ul style="list-style-type: none"> <li>• HCCP is configured and activated.</li> <li>• A modem changes upstream to an DOCSIS 2.0 only channel.</li> </ul> <p>Workaround: Delete the modem and let it come online again.</p>
CSCsi09848	<p>Pagent cannot get a predefined IP DHCP pool so it will automatically be assigned the default. (192.168.100.x).</p> <p>This issue occurs when running HA regression cases.</p> <p>Workaround: Rerun the case.</p>
CSCsi27520	<p>The following interface RPF configuration commands are accepted on theubr10k even though they are not supported in theubr10k microcode:</p> <p><b>ip unicast source reachable-via any allow-default</b></p> <p><b>ip unicast source reachable-via rx &lt;1-199&gt;</b></p> <p><b>ip unicast source reachable-via rx &lt;1300-2699&gt;</b></p> <p>Workaround: Do not configure the unsupported commands.</p>
CSCsi33625	<p>The code automatically changes the acceptable upstream (US) power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This setting is legal for all US channel width options.</p>
CSCsi41787	<p>The <b>show int if downstream</b> CLI shows “cable interface downstream is up” even though the interface is in shutdown state.</p> <p>There are no known workarounds.</p>
CSCsi48608	<p>ACL configured to the CPE is not available after line card/interface switchover.</p> <p>This issue occurs when using <b>cable {modem   host   device} access-group acl</b>.</p> <p>Workaround: Reconfigure ACL to the CPE manually after switchover.</p>
CSCsi81513	<p>HCCP status shows that everything is synced and the Protect is ready for switchover, even though nothing has been synced over and the interdb on the Protect LC is empty.</p> <p>A LC switchover after this is totally broken and modems will never register on the Protect LC</p> <p>This happens only when the Blaze FPGA image is changed for the Modena and is being reprogrammed on CMTS bootup.</p> <p>Workaround: The modems will not register on the modular interface when Blaze FPGA is being reprogrammed. As soon as the Blaze is reprogrammed, reload the CMTS as the modems are already down.</p> <p>On reload everything should work correctly.</p>

**Table 48 Resolved Caveats for Cisco IOS Release 12.3(23)BC (continued)**

DDTS ID Number	Description
CSCsi85054	<p>When dynamic cable modem load balancing is configured between downstream A and downstream B, and downstream B's service flow admission control thresholds are significantly lower than downstream A's. It appears that load balancing still moves modems across to downstream B, even after violating the prescribed Admission control limits.</p> <p>There are no known workarounds.</p>
CSCsi87195	<p>When you configure frequency using SNMP, the range of frequencies accepted is based on the following formula.</p> <pre>min_us_freq = 5000000 + (channel_width/2) max_us_freq = 55000000 - (channel_width/2)</pre> <p>Given a frequency configured, when configuring a channel width that cannot accept the frequency configured already, there should be warning message saying that "channel width cannot be configured with the present frequency".</p> <p>This problem occurs when the frequency you are trying to configure via SNMP is not within the channel width currently configured on the CMTS router.</p> <p>There are no known workarounds.</p>
CSCsj12497	<p>When the <b>cable per-dev-acl</b> command is configured, the access-list assigned to the host is not available after a PRE switchover.</p> <p>There are no known workarounds.</p>
CSCsj12597	<p>As part of OSSI requirement, dot3StatsCarrierSenseErrors need to incremented when the cable is removed from FE Interface. However, this is not happening.</p> <p>There are no known workarounds.</p>
CSCsj14143	<p>The ifHCOctets and ifHCInOctets values retrieved from the IF-MIB are not correct.</p> <p>There are no known workarounds.</p>

**Table 48 Resolved Caveats for Cisco IOS Release 12.3(23)BC (continued)**

DDTS ID Number	Description
CSCsj14502	<p>In certain cases, CMTS does not send intercept packets out in case of cTapStreamIpInterface is set to -1, while other parameters are set correctly in cTapStreamIpTable and snmpwalk show the cTapStreamIpStatus is active.</p> <p>The issue occurs when configuring a cTapStreamIp entry as follows:</p> <pre>cTapStreamIpInterface = -1 cTapStreamIpDestinationAddress = Addr1 cTapStreamIpDestinationLength = 32 cTapStreamIpSourceAddress = Addr2 cTapStreamIpSourceLength = 32</pre> <p>and Addr1 is directly connected to a cable interface, Addr2 is routed through another interface and the net mask of outgoing interface for destination Addr2 is greater than the one of Addr1.</p> <p>Workaround: Perform one of the following:</p> <p>(1) Directly set the tapping interface's IfIndex, letting cTapStreamIpInterface != -1 and != 0</p> <p>(2) or, Either set cTapStreamIpSourceAddress or cTapStreamIpDestinationAddress to zero, to avoid conflict.</p>
CSCsj58093	<p>CPE ping stops after the wideband (WB) switches to the narrowband (NB) mode. This problem occurs when you shut down the WB interface.</p> <p>Workaround: Execute <b>clear arp</b> or <b>clear cable modem</b> commands to clear the ARP entries and then let the cable modem on the NB to come online.</p>
CSCsj61860	<p>When <b>show hccp event-history</b>, it will display twice hccp event log for a hccp event.</p> <p>There are no known workarounds.</p>
CSCsj64207	<p>It seems that the total downstream rate applied to Annex A 256QAM downstreams by admission control is only 1543127 bits per second, as opposed to the real rate which is somewhere around 50Mbps.</p> <p>There are no known workarounds.</p>
CSCsj84440	<p>Adding an RF channel to a WB interface, by configuring <b>cable rf-channel</b> under wideband-cable interface, will cause the corresponding wideband modems to leave w-online state with a "Fiber node x status changed to Invalid state" message shown in CLI.</p> <p>If the RF channel is currently in a fiber node and it is also used by a WB interface, and the fiber node is in a "Valid" state. If this RF channel is added to a new WB interface that does not yet have bundle configured (or a different bundle configured), the fiber node will become "Invalid" due to mismatched bundle number. This will cause the failure of the MD-DS-SG creation and thus WB modem offline.</p> <p>Workaround: Avoid adding a RF channel to a WB interface with a different bundle configuration than the existing one.</p>

**Table 48 Resolved Caveats for Cisco IOS Release 12.3(23)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsk07617	The <b>show cable modem qos</b> command incorrectly shows the original ToS mask after overwrite.  There are no known workarounds.
CSCsk10852	RF channel mismatch error occurs when you run the <b>show hw-module bay association wideband-channel</b> command.  There are no known workarounds.
CSCsk25070	Executing a <b>show packetcable gate summary</b> after oir a cable line card will cause a system crash.  This only occurs at the time hccp is deconfured at the packetcable call are on going in that cable line card.  Workaround: Stop calls before using OIR on the card.
CSCsk28584	Unable to remove the remote query community string.  This issue occurs when un-configuring an invalid remote query community string.  Workaround: Wait for some time after un-configuration and the community string will disappear.
CSCsk28938	On a uBR10k running 12.3(17a)BC and up (and older code, as well), the <b>cable downstream rate-limit</b> command has no affect on DS traffic.  There are no known workarounds.
CSCsk30377	The first show interface service flow count is not correct after pre switchover.  This issue is seen in a uBR10k running 12.3(23)BC.  Workaround: Use show interface service flow count many times, continuously.
CSCsk31357	PCMM gates will not be synced to the standby RP. Hence, if there is a PRE switchover, the newly active RP will not have the PCMM gate information.  This issue occurs when running configuration only has “packetcable multimedia” enabled but not “packetcable”.  Workaround: Enable “packetcable” in running configuration.
CSCsk41698	In the following scenario, if a customer mistakenly configures LC 5/0 as PROTECT, plus the <b>no mem sub x/y revertive</b> command and then corrects the problem by configuring LC 5/1 as PROTECT, the <b>no mem sub x/y revertive</b> command is not reflected in the <b>show hccp detail</b> output.  Workaround: Reconfigure the <b>no mem sub x/y revertive</b> command.
CSCsk52258	An UBR10000-3-INVALID_INVOKE_FROM_ISR error message, along with a traceback, occurs.  In a WB setup, a corner case scenario causes the CM to send a B-INIT-RNG request on a non-broadcast slot and thus causing the invalid invoke from ISR error.  There are no known workarounds.
CSCsk53180	The output of <b>show controllers cx/y/z tech-support</b> contains passwords in the running-configuration. These passwords should be removed, as these tech-support reports are routinely sent to TAC via non-secure email.  There are no known workarounds.

**Table 48** Resolved Caveats for Cisco IOS Release 12.3(23)BC (continued)

DDTS ID Number	Description
CSCsk60014	<p>Symptom: No downstream throughput for PC calls on eMTA accompanied by a warning after a PRE failover. The problem occurs because the standby PRE fails to start its WBCMTS periodic timer after the failover. When the problem occurs wideband capable modems fail to come online in wideband mode and register as narrowband modems instead.</p> <p>Condition: The problem occurs if the failover happens before the Wideband SPA has reached its operational state. This could happen if the card was not inserted prior to the failover. This could also happen if the failover occurred concurrently with downloading the operational firmware. For example, it could happen if the active and standby PREs boot simultaneously and the active PRE is in the process of bringing up the WB SPA when a PRE failover occurs.</p> <p>Workaround: Reload the router.</p>
CSCsk65431	<p>Changing IP add on the int bundle X.1 subinterface results in an Integrated Upconverter flap for all interfaces associated with that bundle.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17)BC or higher that has a bundle interface configured.</p> <p>There are no known workarounds.</p>
CSCsk74917	<p>CMTS crashes.</p> <p>This is a rare situation and only occurs when the current or next element in cm_list_hdr has been deleted by another process during process suspend, and the function does not enough check to ensure the list sanity.</p> <p>There are no known workarounds.</p>
CSCsk99028	<p>Modems flapped and got stuck in init(rc) when there is upstream traffic.</p> <p>Workaround: Do not use load balancing. If load balancing is used, use modem count balancing and let the modems balance and then turn the traffic on. If modems get stuck in init(rc), reset them.</p>

## Open Caveats for Release 12.3(21a)BC4

Table 49 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC4.

**Table 49** Open Caveats for Cisco IOS Release 12.3(21a)BC4

DDTS ID Number	Description
CSCek41611	<p>MC5x20U cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>
CSCek66377	<p>Not all entries are seen for the Protect line card in the MIB table.</p> <p>There are no known workarounds.</p>

**Table 49 Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCek77615	<p>Sometimes the packets/sec value of the Wideband-Cable interface is incorrect and erratic.</p> <p>There are no known workarounds.</p>
CSCek77620	<p>This issue is fixed in 12.3(21)BC4 release through CSCsj31345.</p> <p>Workaround: If you cannot ping modems, try using the <b>clear cable modem reset</b> command and retry running ping for modems.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsd14355	<p>The Simple Network Management Protocol (SNMP)-created quality of service (QoS) profile is not available after a Performance Routing Engine (PRE) switchover; the command- created QoS profile is available after switchover.</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsh19917	<p>Some parent warnings appear when static analysis is performed on the specmib source file.</p> <p>Workaround: No workaround is required. The functionality of the MIB query is not affected.</p>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachable" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachable" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>

**Table 49 Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsh41508	<p>The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.</p> <p>There are no known workarounds.</p>
CSCsh66150	<p>The <b>show cable modem connectivity</b> command output is corrupted under some condition.</p> <p>The following example shows a sample output.</p> <pre data-bbox="574 558 1446 842"> ----- show cable modem connectivity ----- Prim 1st time   Times  %online   Online time           Offline time Sid  online      Online      min    avg    max    min    avg max 9    04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 11   04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00                     </pre> <p>This issue occurs after PRE switchover.</p> <p>Workaround: Clear cable modem delete.</p>
CSCsh69870	<p>The VTMS algorithm has to be optimized due when CMs with different MIRs are mixed. The Downstream can not be fully utilize by a CM configured with a very high MIR (16-20Mbps), even when there is BW available in such Downstream.</p> <p>There are no known workarounds.</p>
CSCsh70679	<p>When sending a trap due to exceeding a threshold, the admission control system fails to report the correct type of event that triggered the threshold to be exceeded.</p> <p>There are no known workarounds.</p>
CSCsh72785	<p>No SNMP trap is generated on behalf of the redundant PRE state change.</p> <p>This issue may occur on the redundant PRE configuration and state change of redundant unit.</p> <p>There are no known workarounds.</p>
CSCsh95096	<p>On a Cisco uBR10012 running Cisco IOS Release 12.3(21)BC, it is possible to change default connector commands even if modems are online on that upstream connector.</p> <p>There are no known workarounds.</p>
CSCsh96105	<p>Under the following conditions, tracebacks are seen and the modem does not come online.</p> <ul data-bbox="574 1629 1308 1703" style="list-style-type: none"> <li>• HCCP is configured and activated.</li> <li>• A modem changes upstream to an DOCSIS 2.0 only channel.</li> </ul> <p>Workaround: Delete the modem and let it come online again.</p>

**Table 49 Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsi05236	<p>When the Ubr10k Half-Height GE linecard is connected to the SCE2000 GE link and both are configured with auto-negotiation, the link does not come up. This problem does not exist for the Full-Height GE.</p> <p>This issue occurs when an Ubr10k Half-Height GE is directly connected to the SCE GE link and auto-negotiation is turned on both links.</p> <p>Workaround: If the auto-negotiation is removed from both GE interfaces, then the link will come up.</p>
CSCsi09848	<p>Pagent cannot get a predefined IP DHCP pool so it will automatically be assigned the default. (192.168.100.x).</p> <p>This issue occurs when running HA regression cases.</p> <p>Workaround: Rerun the case.</p>
CSCsi33625	<p>The code automatically changes the acceptable upstream (US) power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This setting is legal for all US channel width options.</p>
CSCsi41787	<p>The <b>show int if downstream</b> CLI shows “cable interface downstream is up” even though the interface is in shutdown state.</p> <p>There are no known workarounds.</p>
CSCsi48608	<p>ACL configured to the CPE is not available after line card/interface switchover.</p> <p>This issue occurs when using <b>cable {modem   host   device} access-group acl</b>.</p> <p>Workaround: Reconfigure ACL to the CPE manually after switchover.</p>
CSCsi81513	<p>HCCP status shows that everything is synced and the Protect is ready for switchover, even though nothing has been synced over and the interdb on the Protect LC is empty.</p> <p>A LC switchover after this is totally broken and modems will never register on the Protect LC</p> <p>This happens only when the Blaze FPGA image is changed for the Modena and is being reprogrammed on CMTS bootup.</p> <p>Workaround: The modems will not register on the modular interface when Blaze FPGA is being reprogrammed. As soon as the Blaze is reprogrammed, reload the CMTS as the modems are already down.</p> <p>On reload everything should work correctly.</p>

Table 49 Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)

DDTS ID Number	Description
CSCsi83966	<p>Multiple tracebacks are observed:</p> <pre>313861: Apr 10 07:16:06.784 UTC: %REQGRP-3-SYSCALL: System call for command 72 (slot4/0) : Could not send blocked IPC message (Cause: tim- eout) -Traceback= 6069F510 606B35B0 60C5A09C 60C5B7E0 60C58980 61005A70 610093CC 60FF9910 6101FE0C 60916AC4 60916AA8  314045: Apr 10 08:16:39.940 UTC: %REQGRP-3-SYSCALL: System call for command 42 (slot4/0) : Could not send blocked IPC message (Cause: tim- eout) -Traceback= 6069F510 606AC4A8 606AEED4 60C898A0 60C89B34 60C5AD40 60C5B188 60C5B834 60C58980 61005A70 610093CC 60FF9910 6101FE0C 60916AC4 60916AA8  313868: Apr 10 07:18:35.833 UTC: %REQGRP-3-SYSCALL: System call for command 47 (slot4/0) : Could not send blocked IPC message (Cause: tim- eout) -Traceback= 6069F510 606B3D0C 606B4930 6069D1EC 6053BEC4 60886370 60897D40 60916AC4 60916AA8</pre> <p>This issue occurs on a router with an MC28U card. Baseline privacy interface (BPI) and VPN are not configured and no crashinfo is seen on the PRE or line card.</p> <p>Workaround: Reset the affected line card with hardware module stop/start.</p>
CSCsi85054	<p>When dynamic cable modem load balancing is configured between downstream A and downstream B, and downstream B's service flow admission control thresholds are significantly lower than downstream A's. It appears that load balancing still moves modems across to downstream B, even after violating the prescribed Admission control limits.</p> <p>There are no known workarounds.</p>
CSCsi87195	<p>When you configure frequency using SNMP, the range of frequencies accepted is based on the following formula.</p> <pre>min_us_freq = 5000000 + (channel_width/2) max_us_freq = 55000000 - (channel_width/2)</pre> <p>Given a frequency configured, when configuring a channel width that cannot accept the frequency configured already, there should be warning message saying that "channel width cannot be configured with the present frequency".</p> <p>This problem occurs when the frequency you are trying to configure via SNMP is not within the channel width currently configured on the CMTS router.</p> <p>There are no known workarounds.</p>
CSCsj12497	<p>When the <b>cable per-dev-acl</b> command is configured, the access-list assigned to the host is not available after a PRE switchover.</p> <p>There are no known workarounds.</p>
CSCsj12597	<p>As part of OSSI requirement, dot3StatsCarrierSenseErrors need to incremented when the cable is removed from FE Interface. However, this is not happening.</p> <p>There are no known workarounds.</p>

**Table 49 Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsj14502	<p>In certain cases, CMTS does not send intercept packets out in case of cTapStreamIpInterface is set to -1, while other parameters are set correctly in cTapStreamIpTable and snmpwalk show the cTapStreamIpStatus is active.</p> <p>The issue occurs when configuring a cTapStreamIp entry as follows:</p> <pre>cTapStreamIpInterface = -1 cTapStreamIpDestinationAddress = Addr1 cTapStreamIpDestinationLength = 32 cTapStreamIpSourceAddress = Addr2 cTapStreamIpSourceLength = 32</pre> <p>and Addr1 is directly connected to a cable interface, Addr2 is routed through another interface and the net mask of outgoing interface for destination Addr2 is greater than the one of Addr1.</p> <p>Workaround: Perform one of the following:</p> <p>(1) Directly set the tapping interface's IfIndex, letting cTapStreamIpInterface != -1 and != 0</p> <p>(2) or, Either set cTapStreamIpSourceAddress or cTapStreamIpDestinationAddress to zero, to avoid conflict</p>
CSCsj58093	<p>CPE ping stops after the wideband (WB) switches to the narrowband (NB) mode. This problem occurs when you shut down the WB interface.</p> <p>Workaround: Execute <b>clear arp</b> or <b>clear cable modem</b> commands to clear the ARP entries and then let the cable modem on the NB to come online.</p>
CSCsj61860	<p>When <b>show hccp event-history</b>, it will display twice hccp event log for a hccp event.</p> <p>There are no known workarounds.</p>
CSCsj64207	<p>It seems that the total downstream rate applied to Annex A 256QAM downstreams by admission control is only 1543127 bits per second, as opposed to the real rate which is somewhere around 50Mbps.</p> <p>There are no known workarounds.</p>
CSCsj80238	<p>A Cisco router running Cisco IOS Release 12.3(21)BC3 may have voice drop of more than one second after RP switchover.</p> <p>There are no known workarounds.</p>

**Table 49** Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)

DDTS ID Number	Description
CSCsj84440	<p>Adding an RF channel to a WB interface, by configuring <b>cable rf-channel</b> under wideband-cable interface, will cause the corresponding wideband modems to leave w-online state with a “Fiber node x status changed to Invalid state” message shown in CLI.</p> <p>If the RF channel is currently in a fiber node and it is also used by a WB interface, and the fiber node is in a “Valid” state. If this RF channel is added to a new WB interface that does not yet have bundle configured (or a different bundle configured), the fiber node will become “Invalid” due to mismatched bundle number. This will cause the failure of the MD-DS-SG creation and thus WB modem offline.</p> <p>Workaround: Avoid adding a RF channel to a WB interface with a different bundle configuration than the existing one.</p>
CSCsj98444	<p>Although the <b>snmpgetnext</b> command succeeds, the <b>snmpget</b> command returns a “(noSuchName)” error.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17b)BC6 with the Performance Routing Engine 1 (PRE1) and UBR10-MC5X20U-D- CM.</p> <p>There are no known workarounds.</p>
CSCsk07617	<p>The <b>show cable modem qos</b> command incorrectly shows the original ToS mask after overwrite.</p> <p>There are no known workarounds.</p>
CSCsk10852	<p>RF channel mismatch error occurs when you run the <b>show hw-module bay association wideband-channel</b> command.</p> <p>There are no known workarounds.</p>
CSCsk17493	<p>A slow memory leak exists in CR10K Request di and SNMP ENGINE.</p> <p>This issue occurs on a Cisco uBR10000 series (PRE2-RP) router running Cisco IOS Release 12.3(17b)BC4 and the Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCsk28584	<p>Unable to remove the remote query community string.</p> <p>This issue occurs when un-configuring an invalid remote query community string.</p> <p>Workaround: Wait for some time after un-configuration and the community string will disappear.</p>
CSCsk28938	<p>On a uBR10k running 12.3(17a)BC and up (and older code, as well), the <b>cable downstream rate-limit</b> command has no affect on DS traffic.</p> <p>There are no known workarounds.</p>
CSCsk31357	<p>PCMM gates will not be synced to the standby RP. Hence, if there is a PRE switchover, the newly active RP will not have the PCMM gate information.</p> <p>This issue occurs when running configuration only has “packetcable multimedia” enabled but not “packetcable”.</p> <p>Workaround: Enable “packetcable” in running configuration.</p>

**Table 49 Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsk40979	<p>On a Cisco uBR10012 router running 12.3(21a)BC2, the interface mac-scheduler reports higher number of active UGS flows than active calls reported by "show cable calls" for that interface. It also holds the UGS flow BW and do not release. UGS flows are NOT stuck though.</p> <p>The following is an example:</p> <pre>show cable calls reports 2 active UGS calls while mac-scheduler reports 17.</pre> <pre>Router#sh cable modem calls   i 8/1/2/U0 0011.e3ef.6e3d 10.66.50.91 C8/1/2/U0 4029 V - 0011.e3ec.cee2 10.66.52.184 C8/1/2/U0 2143 V</pre> <pre>Router#sh int c8/1/2 mac-scheduler 0 &lt;snip&gt;</pre> <pre>ched Table Adm-State: Grants 17, Reqpolls 0, Util 19% UGS : 17 SIDs, Reservation-level in bps 1543600</pre> <pre>Router#</pre> <p>This issue is only observed when DS load balancing is enable and only on the USs, which are a part of the LB group.</p> <p>There are no known workarounds.</p>
CSCsk41698	<p>In the following scenario, if a customer mistakenly configures LC 5/0 as PROTECT, plus the <b>no mem sub x/y revertive</b> command and then corrects the problem by configuring LC 5/1 as PROTECT, the <b>no mem sub x/y revertive</b> command is not reflected in the <b>show hccp detail</b> output.</p> <p>Workaround: Reconfigure the <b>no mem sub x/y revertive</b> command.</p>
CSCsk41966	<p>a UBR that uses 127.x.x.x prefixes for internal management will include these prefixes in its LDP/TDP address and label mapping messages. Peering routers that have a fix for CSCdx08804 or CSCdx88897 will display error messages like:</p> <pre>%TAGCON-3-TDPID: peer 192.168.254.253:0, TDP Id/Addr mapping problem (rcvd invalid address in TDP address PIE, ignored) %TAGCON-3-TDPID: peer 192.168.254.253:0, TDP Id/Addr mapping problem (rcvd TDP address PIE, bind failed) %TIB-3-REMOTETAG: 127.3.0.0/255.255.0.0, peer 192.168.254.253:0; tag 1; add tag failure</pre> <p>The error messages are harmless. They indicate that the peer has advertised invalid host/network IP addresses, and the receiving router has accordingly ignored the associated advertisements.</p> <p>There are no known workarounds.</p>

Table 49 Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)

DDTS ID Number	Description
CSCsk49540	<p>A line card memory allocation failure is causing a Cisco uBR10000 system slowdown. The <b>show cable modem</b>, <b>show run</b>, and <b>show tech</b> commands all experience noticeable performance slowdowns.</p> <p>This issue occurs because a cable line card is running out of memory; Pool Manager Free shows as 0, and holdong shows a large value.</p> <p>There are no known workarounds.</p>
CSCsk53180	<p>The output of <b>show controllers ex/y/z tech-support</b> contains passwords in the running-configuration. These passwords should be removed, as these tech-support reports are routinely sent to TAC via non-secure email.</p> <p>There are no known workarounds.</p>
CSCsk60014	<p>Symptom: No downstream throughput for PC calls on eMTA accompanied by a warning after a PRE failover. The problem occurs because the standby PRE fails to start its WBCMTS periodic timer after the failover. When the problem occurs wideband capable modems fail to come online in wideband mode and register as narrowband modems instead.</p> <p>Condition: The problem occurs if the failover happens before the Wideband SPA has reached its operational state. This could happen if the card was not inserted prior to the failover. This could also happen if the failover occurred concurrently with downloading the operational firmware. For example, it could happen if the active and standby PREs boot simultaneously and the active PRE is in the process of bringing up the WB SPA when a PRE failover occurs.</p> <p>Workaround: Reload the router.</p>
CSCsk63745	<p>Reduced downstream throughput occurs over time on uBR10k routers with &gt;40000 modems.</p> <p>BE queue aggregation must be taking place for this problem to occur.</p> <p>There are no known workarounds.</p>
CSCsk65431	<p>Changing IP add on the int bundle X.1 subinterface results in an Integrated Up-convertor flap for all interfaces associated with that bundle.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17)BC or higher that has a bundle interface configured.</p> <p>There are no known workarounds.</p>
CSCsk68026	<p>Bus error exception crash on PRE of uBR10k.</p> <p>This issue occurs on an uBR10k with IOS 12.3(21a)BC2, seen on PRE1 as well as PRE2.</p> <p>There are no known workarounds.</p>
CSCsk72430	<p>Increasing docsis frag header discard counters are seen in 12.3(21a)BC3 when running US at high utilization rate. This problems affect multiple CMs.</p> <p>Workaround: Disable docsis frag.</p>
CSCsk72977	<p>If CALEA is enabled in a HA enabled systems, an HA Switchover may crash.</p> <p>Workaround: Do not enable HA when CALEA is being used. Use 12.3(21)BC for CALEA and HA features enabled</p>

**Table 49 Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsk75022	<p>All line card crashes due to IPC timeout.</p> <p>This issue may be due to Ethernet0/0/0 on the PRE has lost carrier count increasing indicates hw issue.</p> <p>There are no known workarounds. However, reload the uBR10k if all line cards crashes and cannot recovered or the UBR10k is acting too slow.</p>
CSCsk85358	<p>This bug is used for back out CSCsk37428</p> <p>This issue occurs when there are many CPE with the same mac-address under one CM.</p> <p>Workaround: Consider the L2VPN/TLS feature in which all CPE traffics are bypassing the CMTS and handled by the upstream router.</p>
CSCsk85395	<p>Low latency flows are allowed to be created that may result in degradation of throughput of other existing flows.</p> <p>There are no known workarounds.</p>
CSCsk86886	<p>A Cisco router running IOS version 123(17b)BC8 may reload unexpectedly.</p> <p>There are no known workarounds.</p>
CSCsk85933	<p>A uBR10k running 12.3(17b)BC3 may report Cable Modems stuck in init(rc) state on certain Upstream Interfaces. Very high number of Input queue drops are also observed under the corresponding Downstream interfaces.</p> <p>This problem has only been observed on uBR10K with MC5x20H-D card.</p> <p>Workaround: Resetting the line card will bring all the Cable Modems back to online.</p>
CSCsk90802	<p>Active PRE2 crashes on an UBR10K chassis running 12.3(17b)BC4 Images with Cable line card. Once this happens, the secondary PRE2 become active.</p> <p>There are no known workarounds.</p>
CSCsk92860	<p>Voice issues, due to excessive packet loss at the time that the router, displays the following error message followed by traceback:</p> <pre data-bbox="613 1346 1430 1371">%GENERAL-3-EREVENT: Unable to write ds_police_rate:ds_rate_limit</pre> <p>This issue occurs uBR10k running 12.3(21)BC.</p> <p>There are no known workarounds.</p>
CSCsk98505	<p>HH-GE's SFP information is missing from the <b>show inventory</b> command.</p> <p>Workaround: The only workaround is physical inspection.</p>
CSCsl06036	<p>Maxcpe functionality is broken with w-online modems. The functionality is working with the same modem in the same image when it registered in the online state.</p> <p>There are no known workarounds.</p>

**Table 49** Open Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)

DDTS ID Number	Description
CSCsl06384	<p>In case where Multiple Working linecards failover at the same time to protect, only one will get protection (a expected). However, one or more LC's will keep trying to get protection and never will go back to steady state (not allowing to bring the CM's back online). The rest of the working cards will be able to get the CM's back online.</p> <p>Service can be restored in these two LC's by shutting down the protect card.</p> <p>Workaround: Disable Keepalive in the Working LC's.</p>
CSCsl10231	<p>A downstream service flow with an associated classifier will have the classifier "match count" initialized to zero if there is a PRE switchover or a reload of the pxf.</p> <p>This issue occurs on a service flow with a classifier and PRE switchover or pxf reload.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(21a)BC4

[Table 50](#) lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC4.

**Table 50** Resolved Caveats for Cisco IOS Release 12.3(21a)BC4

DDTS ID Number	Description
CSCek65425	<p>Seven warnings appear in the getnext docsQoSServiceFlowPkts file.</p> <p>There are no known workarounds.</p>
CSCek76822	<p>The protection LC may unexpectedly reload after Switchover.</p> <p>This issue may only occur when a WB CM with a secondary UGS flow is wb-online during a LC switch over.</p> <p>There are no workarounds.</p>
CSCek78058	<p>Tracebacks may occur on the LC when a submanagement group configuration is changed.</p> <p>This issue only occurs on an ubr10k with IOS 12.3(21a)BC3.</p> <p>There are no known workarounds.</p>

**Table 50 Resolved Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCek79167	<p>The 5x20 CLC crashes when a Sunrise Telecom CM-1000 is configured to act as a cable modem provisioned to do BPI+.</p> <p>This issue is also seen in Cisco IOS Release 12.3(21a)BC2, but not in Cisco IOS Release 12.3(21a)BC1.</p> <p>The following error is seen with debug cable privacy and deb cable bpiapi at the time the BPI auth info packet is received at the CMTS:</p> <pre>Jul 11 15:51:49.714: Root certificate is accepted. Jul 11 15:51:49.718: Success in processing a manufacturer certificate. Jul 11 15:51:49.718: Reading the EURO root cert. Jul 11 15:51:49.746: Failed to open file bootflash:euro-root-cert. Jul 11 15:51:49.746: Failed to open file bootflash:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk0:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk1:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk2:euro-root-cert. Jul 11 15:51:49.746: Failed to open file slot0:euro-root-cert. Jul 11 15:51:49.746: Failed to open file slot1:euro-root-cert.</pre> <p>No euro-cert is install, but root-cert from cable labs is installed on the PRE2's bootflash.</p> <p>There are no known workarounds.</p>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>
CSCsg39288	<p>Backup TCC card may experience a reload (IPCOIR-3-TIMEOUT on TCC card).</p> <p>The issue has been experienced on 12.3(9a)BC9, 12.3(13a)BC2 and 12.3(13a)BC6. There are compare errors in the <b>show controllers clock-reference</b> that do increment. However the clocks are not actually drifting apart, even though the errors are incrementing. Because clocks are not actually drifting, redundancy is not affected, except during the brief period when the backup TCC+ card reloads after a IPCOIR timeout.</p> <p>There are no known workarounds.</p>
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre>SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>

**Table 50 Resolved Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsg75417	<p>On an MC520u card, signal-to-noise ratio (SNR) values might drop on an upstream, which could cause modems to drop offline.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC3 with multiple MC520u cards configured for pre-equalization.</p> <p>Workaround: 1. Disable/enable pre-equalization on the upstream. 2. Change the minislot size.</p>
CSCsh72746	<p>Intermittent bursts of upstream traffic observed on the outgoing WAN interface.</p> <p>This issue occurs with upstream traffic from RF line cards towards WAN interface.</p> <p>There are no known workarounds.</p>
CSCsh91566	<p>Wideband cable modems becomes offline after CMTS is issued <b>microcode reload pxf</b>.</p> <p>This issue occurs when a CMTS that has cable modems registered as wideband cable modems is issued <b>microcode reload pxf</b>. When this happens, all the wideband cable modems go offline as seen in <b>show cable modem</b>.</p> <p>Workaround: This condition is cleared after the wideband interfaces are issued: <b>shutdown</b> <b>no shutdown</b></p>
CSCsh93509	<p>The cable interface hccp configurations are displayed in different order between active and standby RP after RP switchover on N+1.</p> <p>This issue occurs when there are more than two rfswitch-group configured in one hccp group.</p> <p>There are no known workarounds.</p>
CSCsi08976	<p>Some packet cable calls in SA modems are dropped after a line card switchover.</p> <p>This issue occurs when an SA modem, or other type of modems, send a DSC request periodically when a call is ongoing.</p> <p>There are no known workarounds.</p>
CSCsi14167	<p>Dropped calls may occur unexpectedly.</p> <p>There are no know workarounds.</p>
CSCsi73342	<p>The host entries are lost after PRE switchover when command per-dev-acl configured, and any ACL is applied to the host.</p> <p>There are no known workarounds.</p>
CSCsi74026	<p>Multicast traffic that matches MQOS configuration is not forwarded.</p> <p>This condition exists if there is a reload of the PXF while the MQOS configuration is in place.</p> <p>There are no known workarounds.</p>
CSCsi79337	<p>Some Gates are stuck in AUTH state with SFID 0.</p> <p>This issue may occur after multiple N+1 switchover.</p> <p>There are no known workarounds.</p>

**Table 50 Resolved Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsi90691	<p>When all the RF channels are removed from a wideband interface, the BW (bandwidth) shows in the command <b>show interface wide x/y/z:n</b> is not correct. It shows the BW of the last channel removed.</p> <p>There are no known workarounds.</p>
CSCsi91628	<p>After CM reset, SubMgt configuration for that CM is lost.</p> <p>Workaround: Reconfigure the SubMgt parameters.</p>
CSCsi92001	<p>Some packets become stuck in the default queue of the wideband interface and can not be sent out.</p> <p>This issue only occurs when all the RF channels are removed from this wideband interface.</p> <p>There are no known workarounds.</p>
CSCsj10768	<p>The MC5x20h-d line card is frequently crashing with following error in crashinfo file:</p> <pre>Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x604F6C98</pre> <p>There are no known workarounds.</p>
CSCsj27583	<p>Heavy ethernet midplane traffic may cause the midplane ethernet connection to go down, and stay down. This failure will eventually cause an MC520H card crash and reload due to an Inter-Process Communication (IPC) timeout.</p> <p>Workaround: Avoid commands that can cause heavy ethernet traffic on the midplane such as continuous pings or executing the <b>show tech</b> command on MC520H card through a Telnet session.</p> <p>Further Problem Description: The ethernet interrupt will be temporarily disabled under heavy load to give other processes a chance to run. By design, the interrupt should be re-enabled after a short period of time (when a timer expires) or the scheduler finds no processes are ready. The timer is not working on the MC520H card. As a result, the interrupt is disabled for a long time under heavy process load, which in turn causes the IPC timeout.</p>
CSCsj31345	<p>The commit of CSCek77620 had already fixed the problem in geo_cable.</p> <p>Part of the diffs of CSCek77620, which is related to the HCCP function, and inter_cm_instance_t should be committed to the DALI throttle branch to fix this problem in DALI.</p> <p>There are no known workarounds.</p>
CSCsj31629	<p>Wrong subslot in OIR Alarms description printed at log. When alarm source is subslot x/1, it prints subslot 0. Example as:</p> <pre>*Jun 15 17:39:06: %UBR10K_ALARM-6-INFO: ASSERT CRITICAL slot 2/1/0 Active Card \ Removed OIR Alarm - subslot 0</pre> <p>This issue occurs when Real OIR events occurs or the CLI <b>hw-module slot/subslot x/y reset</b> command is executed.</p> <p>There are no known workarounds.</p>

**Table 50 Resolved Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsj42426	<p>A Cisco uBR10000 series router can reset unexpectedly.</p> <p>This issue occurs when using Cisco IOS Release 12.3(21a)BC2 and the Dynamic Shared Secret feature.</p> <p>Workaround: Disable the Dynamic Shared Secret feature.</p>
CSCsj43869	<p>The “map-grant” option should not be included in CLI since “map-grant” can not be seen in upstream direction.</p> <p>There are no known workarounds.</p>
CSCsj43929	<p>When using the cable monitor feature, copies of mac packets are not sent to an external sniffer when used on a per mac-address basis.</p> <p>This issue is seen when using “cable monitor interface &lt;interface_name&gt; mac-address &lt;mac_address of CM&gt; packet-type mac” and is seen on IOS 12.3(13a)BCx / 12.3(17a)BCx / 12.3(21a)BCx</p> <p>There are no known workarounds.</p>
CSCsj47516	<p>A Cisco uBR10000 series router stops generating fast hello packets intermittently, causing the connected remote router to report its neighbor being down due to “Dead timer expired”.</p> <p>This issue is only seen on a Cisco uBR10000 series router that has more than 20 thousand cable modems online and is seen on PRE1, PRE2, and Cisco IOS Releases 12.3(13a)BC6 and 12.3(17a)BC6:</p> <p>Workaround: Disable fast hellos if CMTS has more than 20,000 cable modems and use default OSPF hello timers instead.</p>
CSCsj55318	<p>Show inventory displays old SN of TCCplus after OIR.</p> <p>This issue occurs on an uBR10k with tccplus and running 12.3(21)BC image or 12.3BC image.</p> <p>There are no known workarounds.</p>
CSCsj56262	<p>After customer’s DHCP server is re-configured to provide new/different IP addresses to CMs and EMTAs, when EMTA is restarted it obtains successfully a new IP address from DHCP server. However, afterwards it is not able to download the configuration file from TFTP server. A ping from any host behind CMTS to EMTA is not working, but a ping from CMTS to EMTA’s IP address is working fine.</p> <p>This issue occurs only when <b>cable source-verify</b> is configured under the cable interface.</p> <p>Workaround: Remove <b>cable source-verify</b> from configuration during re-provisioning.</p>
CSCsj60503	<p>If the HH-GigE’s IDPROM does not contain the PID and/or VID value(s), the CMTS will log an error message every 10 seconds.</p> <p>Workaround: Replace the card with one that has valid PID/VID.</p>
CSCsj65794	<p>The netflow table only shows the ingress flows and never the egress.</p> <p>This issue occurs in a uBR10K running 12.3(21)BC.</p> <p>Workaround: Un-configure then reconfigure egress netflow after router reload.</p>

**Table 50 Resolved Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsj70817	<p>The cable filter group match statistics is not correct at upstream.</p> <p>This issue occurs when configuring drop as match action at upstream.</p> <p>There are no known workarounds.</p>
CSCsj70948	<p>The PRE2 crashes and then switches over. When removing, inserting, or switching over the line card redundancy, it crashes when removing the last member of HCCP N+1.</p> <p>This issue occurs on a Cisco uBR10000 series router with PRE2 and Global N+1 Redundancy. When perform removing/inserting the global N+1 member and on the other vty, perform <b>show hccp channel</b> at the same time.</p> <p>Workaround: When perform removing/inserting the hccp global N+1 member:</p> <ol style="list-style-type: none"> <li>1. Only remove the global hccp N+1 member on the same VTY.</li> <li>2. Once the member is removed, only perform the command <b>show hccp brief</b> until the hccp is normalized. for example, no more counters count down from the “show hccp brief” screen</li> <li>3. Wait for 90 seconds, then, it's safe to perform show hccp channel-switch command.</li> </ol> <p>The key is to wait for the HCCP to complete its database. This is rare occurs, but caution should be taken.</p>
CSCsj73475	<p>When SPA is shutdown with “hw-module bay 1/0/1 shut”, CMs on other SPA are disconnected and connected as narrow-band.</p> <p>This issue is seen when SPA, which has configuration or is connected with CMs, is shutdown.</p> <p>Workaround: Before shutting down SPA, remove all configuration for that.</p>
CSCsj73833	<p>With SFP inserted, SFP disappears into entity mib after OIR via <b>hw-module bay</b>.</p> <p>Workaround: Do OIR via <b>hw-module slot</b>.</p>
CSCsj76551	<p>It was observed that the CM transmit levels are dropping +/- 6dB's lower after a undetermined time period when the use of 2 freqs on one connector. The2 US channels are for 2 mac domains:</p> <pre>connector 0 is for US0 of 6/0/0 and US0 of 6/0/4. 6/0/4 U0 is connector 16 by default and a different JIB.</pre> <p>This issue occurs on an uBR10012 running 12.3(13a)BC6 with mc520u with frequency stacking configured on the US.</p> <p>Workaround: Changing the minislots:</p> <pre>From 2 to 4 to 2</pre>
CSCsj76802	<p>From RP Own Errors counter increments in <b>show hard pxf dma count</b> output. This does not affect data/traffic.</p> <p>Spontaneous increments of these counters have been noticed always with no specific side effect.</p> <p>There are no known workarounds.</p>

**Table 50 Resolved Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsj77568	<p>After issuing the <b>test cable ucc</b> command many times, the CM becomes stuck at init(rc). However, it is possible to ping to the CM from uBR10k despite the status init(rc).</p> <p>Workaround: Use <b>clear cable modem &lt;mac-address&gt; delete</b> command.</p>
CSCsj79192	<p>Moving modems using Dynamic Channel Change (DCC) <b>init tech &gt;=1</b> between two upstream channels causes a line card crash when the following configuration exists for the upstream channels in a cable interface:</p> <pre>cable upstream 0 scheduling type ugs mode llq cable upstream 1 scheduling type ugs mode llq</pre> <p>This issue can occur when the CMTS is configured for load balance or some general DCC testing is in progress.</p> <p>Workaround: If you remove the following line from the upstream configuration, the LC crash will not occur:</p> <pre>cable upstream 0 scheduling type ugs mode llq</pre>
CSCsj81788	<p>With a SA cable modem, Call drops occur when doing Linecard switchover.</p> <p>There are no known workarounds.</p>
CSCsj84978	<p>Persistent PCMM gates have SFID of 0.</p> <p>This issue occurs after N+1 switchover.</p> <p>Workaround: The Policy Server needs to send GATE-SET again.</p>
CSCsj85484	<p>A Cisco uBR10000 series (PRE2-RP) router running Cisco IOS Release 12.3(21)BC crashes with tracebacks when issuing several <b>cable intercept</b> commands.</p> <p>There are no known workarounds.</p>
CSCsj93582	<p>The voice flows are not in LLQ.</p> <p>This issue occurs on packetcable voice calls.</p> <p>There are no known workarounds.</p>
CSCsj93625	<p>Potential data corruption may occur when using the following:</p> <p>CLI command: show hw-module bay 1/0/0 association wideband-channel</p> <p>There are no known workarounds.</p>
CSCsk01229	<p>Dynamic Secret becomes all zeros after line card switchover.</p> <p>Workaround: Delete CM after LC switchover.</p>
CSCsk03541	<p>When using the cable monitor feature for certain cable interfaces, copies of the map-grant packets are not sent to a WAN interface when used on a per service identifier (SID) basis with the Cablevision configuration/setup.</p> <p>This issue occurs in Cisco IOS Release 12.3(21a)BC and later releases when using the <b>cable monitor outbound interface interface-name sid sid-# packet-type mac type map-grant</b> command.</p> <p>Workaround: Do not use the atdma setting in the cable interface.</p>

**Table 50 Resolved Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

DDTS ID Number	Description
CSCsk04297	<p>The <b>clear cable modem wideband regis reset</b> command will not clear the Cooper CM.</p> <p>This issue only occurs under some special conditions, such as when the wideband channels are not configured or when the CM received none-primary MDD and primary MDD at the same channel.</p> <p>There are no known workarounds.</p>
CSCsk06164	<p>Some specific cable modems cannot come online(pt).</p> <p>The Manufacturer certificate is self-signed and not Docsis compliant. Therefore the CMTS drops the certificate.</p> <p>There are no known workarounds.</p>
CSCsk26038	<p>The output of <b>show pxf cable feature-table</b> needs to be reformatted in order to accommodate the Wideband and Modular Cable interfaces and the bundle sub-interfaces.</p> <p>There are no known workarounds.</p>
CSCsk26979	<p>Dynamic Message Integrity Check (DMIC) may run into an infinite loop, essentially becoming a CPUHOG that brings the router to a software-forced crash.</p> <p>This issue occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(17b)BC08 when DMIC is enabled.</p> <p>Workaround: Disable DMIC.</p>
CSCsk31534	<p>After a LC failover triggered by keepalive timeouts, the WORKING linecard fails over to the PROTECT. While on PROTECT, the cable modems do not get an IP address and does not come back online.</p> <p>This issue is only seen if the global HA “configuration” option is configured. If the global HA “configuration” option is not configured, everything works as expected.</p> <p>There are no known workarounds.</p>
CSCsk32615	<p>The ip mroute cache can be disabled in the bundle interface, which is not expected.</p> <p>There are no known workarounds.</p>
CSCsk46683	<p>The following debug code was added to debug Inter-Process Communication (IPC) timeout problems in customer networks:</p> <ol style="list-style-type: none"> <li>1. The ipc timeout err code was split into the following specific error codes: ack buf/protocol timeout, rsp timeout, and nack timeout.</li> <li>2. The log error message was added to all the places where msg send returns errors.</li> <li>3. The log error message was added to all the places where msg enqueue fails.</li> <li>4. To debug an RPC timeout, a timestamps field was added in the cr10k request-msgs, and a check of the time elapsed at different points along the rpc msg route was added.</li> </ol> <p>Enhancements were added to all the IPC timeout-related error messages to display more info, including cpu usage and KA msgs tx/rx timestamps.</p>

**Table 50 Resolved Caveats for Cisco IOS Release 12.3(21a)BC4 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsk49655	Wideband interface with <b>shutdown</b> CLI configured will become “UP” after PRE switchover. There are no known workarounds.
CSCsk51500	Simultaneous snmpwalks stops due to an “oid not increasing” error. Workaround: Turn off cable snmp cache engine.
CSCsk54166	This caveat is to fix an error introduced in CSCsk46683. There are no known workarounds.
CSCsk55171	<b>show cable modem cable x/x/x access-group</b> does not work correctly. This issue occurs in anubr10k with IOS 12.3(21a)BC2. There are no known workarounds.
CSCsk59432	After a PRE switchover, wideband modems hosted on a 520 linecard, that is also configured as the SPA modular-host, may go offline and then come back online. This also includes wideband modems that are currently registered as narrowband. This issue occurs in 12.3(21)BC. There are no known workarounds.
CSCsk61382	Memory leak occurs with enable device trap This issue occurs with enable device trap of A then generate device trap B. Workaround: Disable all device trap.
CSCsk66396	Inter-Process Communication (IPC) may be slower or the 5x20 protect line card CPU usage may near 100% for the CMTS cm-onoff trap process. There are no known workarounds.
CSCsk77260	DSA-REQ gets rejected. This issue occurs when Poll-Jitter is multiple integral of grant-interval in the UGS-AD flowspec of a DSA-REQ. Workaround: Turn off silence suppression
CSCsk87705	Windows PC rejects the DHCP IP address. There are no known workarounds.

## Open Caveats for Release 12.3(17b)BC9

Table 51 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC9.

**Table 51** Open Caveats for Cisco IOS Release 12.3(17b)BC9

DDTS ID Number	Description
CSCej52423	<p>The wrong number of bytes are suppressed and packet drops occur on the dial shelf controller (DSC) when adding payload header suppression (PHS) and line card (LC) switchover.</p> <p>This issue occurs when performing a switchover while using LC redundancy and Multiple PHS for a secondary service flow (SF).</p> <p>Workaround: Do not use PHS with multiple rules for an SF if you are using N+1.</p>
CSCek23320	<p>Simple Network Management Protocol (SNMP)-related traceback occurs when the image is loaded with the attached cable modem termination system (CMTS) configuration:</p> <pre>*Dec 21 16:11:28.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/1, changed state to up Dec 21 16:12:08.141: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61156234 reading 0x0 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 61156234 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 6115623C 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:14:11.138: %AAAA-3-DROPACCTSNDFAIL: Accounting record dropped, send to server failed: system-start There are no known workarounds.</pre>
CSCek24075	<p>Zero nodes are reported in the <b>show srp topology</b> command.</p> <p>There are no known workarounds.</p>
CSCek27678	<p>The <b>show access-list</b> command displays the access control lists (ACLs) for deleted packet filter groups. The corresponding internal ACLs are not removed, even after the packet filter group is deleted.</p> <p>The <b>show cable filter</b> command lists the reserved ACL group 255 index 1 with drop action, even if all the cable filter configurations have been removed from the cable modem termination system (CMTS).</p> <p>There are no known workarounds.</p>
CSCek31526	<p>The Inter-Process Communication (IPC) between cable line cards occasionally fails.</p> <p>Workaround: Reload the image to fix this issue.</p>
CSCek38598	<p>No corresponding parallel express forwarding (PXF) queue is created for the new dynamic service flow when testing the dynamic service messaging (DSX) with the <b>test cable DSA</b> command.</p> <p>The real Media Terminal Adapters (MTAs) are able to make call with DSX without any problem.</p> <p>There are no known workarounds.</p>

Table 51 Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)

DDTS ID Number	Description
CSCek39428	DC Directory (DCD) messages do not get captured if the <i>mac-address</i> parameter is specified in the <b>cable monitor</b> command. There are no known workarounds.
CSCek41611	Cisco uBR10-MC5X20U cards may experience a silent reload. This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2. There are no known workarounds.
CSCek42764	After a line card switchover, the working standby interface configuration is displayed in the <b>show dsgr tunnel</b> output. Workaround: Skip the standby interface when scanning cable interfaces to display the DOCSIS Set-Top Gateway (DSG) tunnel information.
CSCek66377	Not all entries are seen for the Protect line card in the MIB table. There are no known workarounds.
CSCsa64533	The default modulation profiles for the MC5x20 line card are not optimized for Voice over IP (VoIP). If the intent is to run PacketCable VoIP with G711 at 20 msec packetization without payload header suppression (PHS), the current default modulation profiles can be very inefficient. Workaround: Perform the following steps: <ol style="list-style-type: none"> <li>1. Instead of profile 21, configure profile 22.</li> <li>2. Change the FEC CW size to 232.</li> <li>3. Change the FEC T bytes to 9.</li> <li>4. Repeat these steps for profiles 121 and 221.</li> </ol> Note that other line cards, such as the MC28U, already have optimized modulation profiles.
CSCsb21856	Spectrum groups with discrete frequency entries are not supported on cable line cards containing Advanced Spectrum Management functionality. A warning message should be generated if such a spectrum group is applied to an Advanced Spectrum Management capable upstream port. There are no known workarounds.

**Table 51**      **Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)**

DDTS ID Number	Description
CSCsb29361	<p>In some circumstances, a cable modem with a downstream minimum reserved rate is allowed to register on a Cisco uBR10000 series cable modem termination system (CMTS). However, committed information rate (CIR) resources for the modem are not available. Error messages similar to the following are displayed in the unit's log:</p> <pre data-bbox="613 489 1528 594">%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow 236, CM 0004.9e95.f2a9</pre> <p>The modem is not able to receive any downstream data.</p> <p>The issue occurs only when the total reserved downstream bandwidth approaches the total available downstream bandwidth.</p> <p>There are no known workarounds.</p>
CSCsc12507	<p>When PacketCable event messaging is enabled, the cable modem termination system (CMTS) always uses the global routing table to find the route for the dynamically learned record keeping server (RKS) address. As a result, if the RKS IP address is part of a VPN routing/ forwarding (VRF) route table, CMTS fails to do the correct routing for the Remote Authentication Dial-In User Service (RADIUS) accounting messages.</p> <p>This issue occurs on a Cisco uBR10012 CMTS with a Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) based setup.</p> <p>Workaround: Perform a controlled route distribution between the VRF routing table and the global routing table so that the route for RKS server will be available on the global IPV4 routing table.</p>
CSCsc30294	<p>The following traceback occurs when testing line card failover while making a call from a Cisco uBR10000 series router.</p> <pre data-bbox="613 1224 1528 1350">Remote CMTS calls in progress CLI switchover working to protect. SLOT 5/0: Oct 25 17:25:20.871: %SCHED-3-STUCKMTMR: Sleep with expired managed timer 62B2ABD4, time 0xE06B58 (00:00:00 ago). -Process= "Dynamic Services Timer Process", ipl= 4, pid= 40 -Traceback= 601306F0 60130B48 60283108</pre> <p>There are no known workarounds.</p>
CSCsc38875	<p>When a downstream cable interface on a Cisco uBR series router cable modem termination system (CMTS) experiences sustained congestion, and a significant portion of the downstream traffic is multicast traffic, Internet Group Management Protocol Version 2 (IGMPv2) Query messages might not be transmitted successfully in the downstream direction on that cable interface.</p> <p>The issue occurs when large volumes of multicast traffic, using groups that are not specified, use the cable interface <b>cable match address</b> command.</p> <p>Workaround: Ensure that all multicast traffic passing through the CMTS is classified with an appropriate <b>cable match address</b> command. This workaround may be effective only on Cisco uBR10000 series routers.</p>

**Table 51** Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)

DDTS ID Number	Description
CSCsc81321	<p>The <b>vendor</b> option is missing from the <b>show cable modem</b> command. When specifying an interface, such as <b>show cable modem c4/0 vendor</b>, the <b>vendor</b> option does not work.</p> <p>Workaround: Use a command without a specific interface to get all interfaces, such as the <b>show cable modem vendor</b> command.</p>
CSCsc91717	<p>There is a discrepancy in packet classification between the Fast Ethernet and Gigabit Ethernet interfaces.</p> <p>There are no known workarounds.</p>
CSCsd03740	<p>The <b>cable upstream 0 scheduling type?</b> command is not synchronized during N+1 switchover.</p> <p>There are no known workarounds.</p>
CSCsd31970	<p>On a Cisco uBR10000 series cable modem termination system (CMTS) with redundant Performance Routing Engine (PRE) modules, new interface mode configuration commands entered on the active PRE may not be properly synchronized to the standby PRE if the <b>do show running-configuration</b> command is entered in interface configuration mode.</p> <p>This may lead to a configuration mismatch between the two PRE modules, and may cause difficulty on PRE switchover.</p> <p>Workaround: Refrain from issuing the <b>do show running-configuration</b> command in interface configuration mode, or completely exit interface configuration mode after issuing the command.</p>
CSCsd36652	<p>When configuring line card redundancy by using the <b>global HA</b> commands, duplicate RF-switch slot numbers were configured. This configuration is not allowed.</p> <p>There are no known workarounds.</p>
CSCsd43741	<p>VID data in the entPhysicalHardwareRev MIB displays the wrong value if the data field in EEPROM is missing.</p> <p>This issue affects the Entity MIB in all Cisco uBR10000 software releases, if the VID data field is not programmed.</p> <p>There are no known workarounds.</p>
CSCsd44373	<p>Certain upstream (US) parameters are not copied from a Working cable line card (CLC) to the Protect CLC during a failover under the following conditions: -upstream docsis mode, -upstream modulation profile, -upstream data-backoff.</p> <p>Because the original settings on the Protect CLC remain, it is possible after a failover to have a Data-over-Cable Service Interface Specification (DOCSIS) mode and modulation profile inconsistent with that of the Working CLC prior to the failover. This inconsistency can create problems. For example, if a Time Division Multiple Access (TDMA)-only Working CLC fails over to a Protect CLC configured with Asynchronous Time Division Multiple Access (ATDMA), the cable modems will switch to ATDMA mode. When the Protect fails back to the TDMA-only Working CLC, the cable modems will continue to use ATDMA and lose IP connectivity.</p> <p>There are no known workarounds.</p>

**Table 51**      **Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)**

DDTS ID Number	Description
CSCsd77991	<p>A line card on the Cisco uBR10000 series router unexpectedly crashes.</p> <p>This issue occurs when the <b>clear cable modem</b> command is executed for multicast address.</p> <p>Workaround: Do not use the <b>clear cable modem</b> command for multicast addresses.</p>
CSCsd78370	<p>The privacy bit value of the Multicast entries present on the cable modem termination system (CMTS) host database change after a Route Processor Redundancy (RPR) switchover.</p> <p>This issue occurs when adding multicast entries into the CMTS host database but before the RPR Switchover.</p> <p>There are no known workarounds.</p>
CSCsd95113	<p>A cable modem, when enforced with a quality of service (QoS) profile created using the cdxCmtsCmQosProfile MIB, accepts the profile and <b>show cable modem reg</b> shows the modem with the enforced profile. However, the same cable modem, after reset, does not come online with the enforced profile. Instead, it comes online with the default profile. In contrast, the same modem (when enforced with the QoS profile created using the CLI) comes online after reset with the enforced profile, not the default profile.</p> <p>This behavior is the same irrespective of platforms and whether the QoS profile is created using the CLI or Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCse00902	<p>Various <b>show</b> commands use improper case and spelling.</p> <p>There are no known workarounds.</p>
CSCse02543	<p>When some modems are in the reject state and a <b>clear cable modem reject delete</b> command is issued, a CM_INCONSISTENCY message is generated.</p> <p>Workaround: Do not use the <b>clear cable modem reject delete</b> command.</p>
CSCse43344	<p>When a lockout of the Working card is followed by online insertion and removal (OIR), the following two problems occur: 1) OIR switches from the Working card to the Protect card, dropping all the cable modems. 2) After the Working card is back from the OIR, traffic stays on the Protect card with the cable modems down, and the Working card has lockout active. Clearing lockout fails, and because the Working card is standby, reverting to the Working card would also fail.</p> <p>There are no known workarounds.</p>
CSCse45342	<p>Configuring cable default-tos-qos10 tos-overwrite and resetting the modem does not create a new qos-profile. The modem comes online with the existing profile.</p> <p>The problem occurs on modems provisioned in Data-over-Cable Service Interface Specification (DOCSIS) 1.0 mode when the default tos-mask and tos-value are configured.</p> <p>There are no known workarounds.</p>

Table 51 Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)

DDTS ID Number	Description
CSCse54378	<p>On a Cisco uBR10000 series router running Cisco IOS image ubr10k-k9p6u2-mz.2006-06-02.123_17_BC, tracebacks are found at sch_rp_download_debug_info when you attempt to configure an already assigned address.</p> <p>There are no known workarounds.</p>
CSCse67808	<p>The cdpCacheTable contains entries with index 4294967295 that are only available using the Simple Network Management Protocol (SNMP) <b>get-next</b> command. When the <b>get-one</b> command is used to retrieve the same value, the NO_SUCH_INSTANCE_EXCEPTION is returned.</p> <p>This issue appears to be related to the management ethernet port on the secondary Performance Routing Engine (PRE) in a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCse67868	<p>The Simple Network Management Protocol (SNMP) cpmCPUTotalPhysicalIndex object returns valid entPhysicalIndex values for cable line cards when these values are retrieved using the <b>getnext</b> command, but when the <b>getone</b> command is used, the physical index values for the cable line cards (CLCs) are returned as 0.</p> <p>This issue occurs on Cisco uBR10000 series routers with cable line cards and SNMP configured.</p> <p>There are no known workarounds.</p>
CSCse78143	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>show cr10k-rp cable x/y/z sid</b> command does not allow the service identifier (SID) value to be set to values greater than 8176. As a result, queues associated with downstream multicast quality of service (QoS) SIDs cannot be examined.</p> <p>There are no known workarounds.</p>
CSCse80641	<p>The Transparent LAN Service (TLS) feature does not support stacked dot1q tags. This condition occurs when the TLS feature is configured, and the cable modem termination system (CMTS) receives a 1522 bytes packet (including the frame check sequence(FCS)) in the upstream direction that contains an 802.1q tag.</p> <p>There are no known workarounds.</p>
CSCse84566	<p>This is a feature request for enhancing the Admission Control error messages to help analyze complex system test under heavy PC calls for long period of time.</p>

**Table 51**      **Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)**

DDTS ID Number	Description
CSCse85188	<p>On a Cisco cable modem termination system (CMTS), the quality of service (QoS) profile value for the maximum downstream burst is not displayed correctly and may not be set correctly after a reload.</p> <p>This issue occurs when the maximum downstream burst for a QoS profile is configured using the <b>cable qos profile n max-ds-burst value</b> command with a <i>value</i> greater than 2147483647. The value will be displayed as a negative number in the <b>show run</b> command output. If the configuration is written to memory, the maximum downstream burst is also saved as a negative number. As a result, this value is not processed correctly when the configuration is processed after a reload.</p> <p>There are no known workarounds. (Note that the <b>cable qos profile</b> command has been deprecated for Data-over-Cable Service Interface Specification (DOCSIS) 1.1 use because DOCSIS 1.1 replaces the QoS profile with a service flow, which is configured using the <b>cable service class</b> command.</p>
CSCse88914	<p>The total of exclusive bandwidth allocated to various service class names of a particular scheduling type exceeds the exclusive allocation configured for that scheduling type.</p> <p>There are no known workarounds.</p>
CSCsf04338	<p>The Cisco uBR series cable modem termination system (CMTS) with cable or bundle subinterfaces configured does not prevent customer premises equipment (CPE) from receiving a Dynamic Host Configuration Protocol (DHCP) offer with an IP address belonging to the wrong subinterface. Only DHCP offers that contain an offered IP address within the same subinterface as the cable modem belonging to the customer premises equipment (CPE) should be forwarded by the CMTS.</p> <p>The issue occurs when the CMTS is configured to use cable or bundle subinterfaces and the DHCP server is misconfigured.</p> <p>Workaround: Ensure that the DHCP server is configured to assign CPE devices IP addresses from only the appropriate IP subnets.</p>
CSCsf22037	<p>The cable sflog maximum entry value needs to be changed to 1-59999</p> <p>There are no known workarounds.</p>
CSCsf30877	<p>The wrong classification is applied to the IP Protocol field.</p> <p>There are no known workarounds.</p>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>

Table 51 Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)

DDTS ID Number	Description
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre>SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>
CSCsg74219	<p>When N+1 line card switchover happens in a Cisco uBR10000 series router running Cisco IOS Release 12.3(21)BC, it is possible that dhcp source verification requests may be sent out again, even though the verification has already been performed before the switchover.</p> <p>This issue occurs when the <b>cable source verify dhcp</b> command is configured on the cable interface on a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCsg75417	<p>On an MC520u card, signal-to-noise ratio (SNR) values might drop on an upstream, which could cause modems to drop offline.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC3 with multiple MC520u cards configured for pre-equalization.</p> <p>Workaround: 1. Disable/enable pre-equalization on the upstream. 2. Change the minislot size.</p>
CSCsh20158	<p>On a Cisco uBR series cable modem termination system (CMTS), if the <b>cable source-verify dhcp</b> function receives a NAK in response to a Dynamic Host Configuration Protocol (DHCP) leasequery, it stops sending any more leasequeries until the system performs a successful DHCP release/renew.</p> <p>This issue could potentially stop a legitimate user from getting connectivity for a short period of time.</p> <p>There are no known workarounds.</p>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachables" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachables" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>

**Table 51** *Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh40400	<p>Lower throughput rates occur when the default upstream (US) setting of "token bucket rate limiting with shaping" is enabled.</p> <p>This issue seems to occur because the shaping is causing the rate limiting to kick in too early, resulting in premature delayed grants, and reduced bandwidth.</p> <p>Workaround: Disable shaping and only use token bucket rate limiting if you want to achieve high throughputs in the US.</p>
CSCsh69870	<p>The VTMS algorithm has to be optimized when cable modems (CMs) with different MIRs are mixed. The downstream can not be fully utilize by a CM configured with a very high MIR (16-20Mbps), even when there is bandwidth available in the downstream.</p> <p>There are no known workarounds.</p>
CSCsh72746	<p>Intermittent bursts of upstream traffic observed on the outgoing WAN interface.</p> <p>This issue occurs with upstream traffic from RF line cards towards WAN interface.</p> <p>There are no known workarounds.</p>
CSCsh72785	<p>No SNMP trap is generated on behalf of the redundant PRE state change.</p> <p>This issue may occur on the redundant PRE configuration and state change of redundant unit.</p> <p>There are no known workarounds.</p>
CSCsi30772	<p>After an upgrade from Cisco IOS Release 12.2BC to Cisco IOS Release 12.3BC, the Packetcable code may start rejecting DSA-Req explicitly containing the poll jitter TLV.</p> <p>Workaround: Either drop the poll jitter altogether or use Cisco IOS Release 12.2BC.</p>
CSCsi33625	<p>The code automatically changes the acceptable upstream (US) power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This setting is legal for all US channel width options.</p>

Table 51 Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)

DDTS ID Number	Description
CSCsi83966	<p>Multiple tracebacks are observed:</p> <pre>313861: Apr 10 07:16:06.784 UTC: %REQGRP-3-SYSCALL: System call for command 72 (slot4/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 6069F510 606B35B0 60C5A09C 60C5B7E0 60C58980 61005A70 610093CC 60FF9910 6101FE0C 60916AC4 60916AA8  314045: Apr 10 08:16:39.940 UTC: %REQGRP-3-SYSCALL: System call for command 42 (slot4/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 6069F510 606AC4A8 606AEED4 60C898A0 60C89B34 60C5AD40 60C5B188 60C5B834 60C58980 61005A70 610093CC 60FF9910 6101FE0C 60916AC4 60916AA8  313868: Apr 10 07:18:35.833 UTC: %REQGRP-3-SYSCALL: System call for command 47 (slot4/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 6069F510 606B3D0C 606B4930 6069D1EC 6053BEC4 60886370 60897D40 60916AC4 60916AA8</pre> <p>This issue occurs on a router with an MC28U card. Baseline privacy interface (BPI) and VPN are not configured and no crashinfo is seen on the PRE or line card.</p> <p>Workaround: Reset the affected line card with hardware module stop/start.</p>
CSCsi87821	<p>Cable modems may re-range with pre-equalization enabled.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17b)BC4 with MC520U cards and pre-equalization enabled.</p> <p>Workaround: Disable pre-equalization.</p>
CSCsj20998	<p>The crashinfo file of the Cisco uBR10000 series router may be incomplete. Extra information that is used for debugging unexpected reloads may not be included in the crashinfo file.</p> <p>There are no known workarounds.</p>
CSCsj30057	<p>The CMTS responds slowly to the CLI until the MC520U line card is reset through the CLI.</p> <p>The MC520U line card may reset due to the following:</p> <pre>%REQGRP-3-SYSCALL: System call for command 43 (slot6/0) : Nonblocking request failed (Cause: timeout)</pre> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17b)BC4 .</p> <p>Workaround: Reset the line card through the CLI.</p>
CSCsj36054	<p>The link LED on HH-1GE remains green despite issuing the <b>shutdown</b> command. The link LED also remains green despite disconnecting the fiber cable.</p> <p>These issues are seen on Cisco IOS releases 12.3(13a)BC6, 12.3(21a)BC1 or 12.3(21a)BC2 with PRE2 with a Half-Height Gigabit Ethernet Line Card on slot3/0 or 4/0.</p> <p>There are no known workarounds.</p>

**Table 51**      **Open Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsj98444	<p>Although the <b>snmpgetnext</b> command succeeds, the <b>snmpget</b> command returns a "(noSuchName)" error.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17b)BC6 with the Performance Routing Engine 1 (PRE1) and UBR10-MC5X20U-D- CM.</p> <p>There are no known workarounds.</p>
CSCsk17493	<p>A slow memory leak exists in CR10K Request di and SNMP ENGINE.</p> <p>This issue occurs on a Cisco uBR10000 series (PRE2-RP) router running Cisco IOS Release 12.3(17b)BC4 and the Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCsk37428	<p>Static IP customers behind a Private Internet EXchange (PIX) firewall connected to the cable modem lose IP connectivity after a Hot Standby Connection-to-Connection Protocol (HCCP) switchover. The failure can occur after a switchover from Working to Protect or vice versa.</p> <p>This issue occurs on a Cisco uBR10000 series router a with Performance Routing Engine 1 (PRE2) running Cisco IOS Release 12.3(17b)BC4 when the Static IP customers are connected to the inside interface of a PIX firewall and the outside interface is connected to the cable modem.</p> <p>Workaround: Clear the ARP entries on the CMTS for the associated IP addresses, or remove the affected secondary IP subnet from the bundle or cable interface configuration and then re-add it.</p> <p>Further Problem Description: This issue can also occur in Cisco IOS Release 12.3(21a)BC3. Note that the affected IP addresses may be ping-able from the CMTS (sourced from the cable or the GigE interface), but not from an upstream router.</p>
CSCsk49540	<p>A line card memory allocation failure is causing a Cisco uBR10000 system slowdown. The <b>show cable modem</b>, <b>show run</b>, and <b>show tech</b> commands all experience noticeable performance slowdowns.</p> <p>This issue occurs because a cable line card is running out of memory; Pool Manager Free shows as 0, and holdong shows a large value.</p> <p>There are no known workarounds.</p>
CSCsk65431	<p>Changing IP add on the int bundle X.1 subinterface results in an Integrated Upconverter flap for all interfaces associated with that bundle.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17)BC or higher that has a bundle interface configured.</p> <p>There are no known workarounds.</p>
CSCsk66396	<p>Inter-Process Communication (IPC) may be slower or the 5x20 protect line card CPU usage may near 100% for the CMTS cm-onoff trap process.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(17b)BC9

Table 52 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC9.

**Table 52** Resolved Caveats for Cisco IOS Release 12.3(17b)BC9

DDTS ID Number	Description
CSCed95187	<p>RST packets may contain a non-randomized identification value on the IP header.</p> <p>This issue is observed on a Cisco platform that receives a TCP SYN packet on a non-listening port.</p> <p>There are no known workarounds.</p>
CSCeh48684	<p>Identification field is always 0 in the tacacs+ packet with SYN flag. The tacacs packet goes from a cat6509 through a FW to the AAA server. The FW construes this as a Fragment Overlap Attack and drops additional new connections.</p> <p>There are no known workarounds.</p>
CSCek79167	<p>The 5x20 CLC crashes when a Sunrise Telecom CM-1000 is configured to act as a cable modem provisioned to do BPI+.</p> <p>This issue is also seen in Cisco IOS Release 12.3(21a)BC2, but not in Cisco IOS Release 12.3(21a)BC1.</p> <p>The following error is seen with debug cable privacy and deb cable bpiapi at the time the BPI auth info packet is received at the CMTS:</p> <pre> Jul 11 15:51:49.714: Root certificate is accepted. Jul 11 15:51:49.718: Success in processing a manufacturer certificate. Jul 11 15:51:49.718: Reading the EURO root cert. Jul 11 15:51:49.746: Failed to open file bootflash:euro-root-cert. Jul 11 15:51:49.746: Failed to open file bootflash:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk0:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk1:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk2:euro-root-cert. Jul 11 15:51:49.746: Failed to open file slot0:euro-root-cert. Jul 11 15:51:49.746: Failed to open file slot1:euro-root-cert.                     </pre> <p>No euro-cert is install, but root-cert from cable labs is installed on the PRE2's bootflash.</p> <p>There are no known workarounds.</p>
CSCsg39288	<p>Backup TCC card may experience a reload (IPCOIR-3-TIMEOUT on TCC card).</p> <p>The issue has been experienced on 12.3(9a)BC9, 12.3(13a)BC2 and 12.3(13a)BC6. There are compare errors in the <b>show controllers clock-reference</b> that do increment. However the clocks are not actually drifting apart, even though the errors are incrementing. Because clocks are not actually drifting, redundancy is not affected, except during the brief period when the backup TCC+ card reloads after a IPCOIR timeout.</p> <p>There are no known workarounds.</p>

**Table 52** *Resolved Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsg75417	<p>On an MC520u card, signal-to-noise ratio (SNR) values might drop on an upstream, which could cause modems to drop offline.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC3 with multiple MC520u cards configured for pre-equalization.</p> <p>Workaround: 1. Disable/enable pre-equalization on the upstream. 2. Change the minislot size.</p>
CSCsg81866	<p>Traffic to the active Protect card stops, and the interface reverts back to the original Working card.</p> <p>This issue can occur in the following scenario:</p> <ol style="list-style-type: none"> <li>1. The configured connector setting on the Protect card is not a mirror of all Working cards.</li> <li>2. The Protect line card is currently active.</li> <li>3. The active Protect card receives syncs from Working cards that have different connector configurations, and a map interrupt on the active interface on the Protect card operates on an erroneous connector setting, resulting in a stuck upstream on the active Protect interface. At this point, if auto revert is configured, the CMTS reverts back to the original Working interface.</li> </ol> <p>Workaround: Configure all connector settings to be the same.</p>
CSCsh92986	<p>The latency for the <b>RS</b>H command could increase when they are flowing through an FWSM module.</p> <p>The following issue was observed on an FWSM that is running 2.2 software: (1) The long delay was triggered by using either Cisco IOS Release 12.3(13a)BC1 or (2) Release 12.3(17a)BC1 on routers toward which those RSH commands were sent.</p> <p>Workaround: Either bypass the FWSM module or downgrade to Cisco IOS Release 12.3(9a)BC3, which is not affected by this extra delay issue.</p>
CSCsj10768	<p>The MC5x20h-d line card is frequently crashing with following error in crashinfo file:</p> <pre>Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x604F6C98</pre> <p>There are no known workarounds.</p>
CSCsj16292	<p>Following an upgrade to Cisco IOS Release 12.2(18)SXF9, the following message may be displayed:</p> <pre>%DATACORRUPTION-1-DATAINCONSISTENCY: copy error -Traceback=</pre> <p>This message may appear as a result of Simple Network Management Protocol (SNMP) polling of PAgP variables, but does not appear to be service impacting.</p> <p>There are no known workarounds.</p>

Table 52 Resolved Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)

DDTS ID Number	Description
CSCsj18014	<p>A caller ID may be received with extra characters.</p> <p>This issue is observed when caller ID is enabled on both routers and when the station ID and station name are configured on the FXS side.</p> <p>There are no known workarounds.</p>
CSCsj27583	<p>Heavy ethernet midplane traffic may cause the midplane ethernet connection to go down, and stay down. This failure will eventually cause an MC520H card crash and reload due to an Inter-Process Communication (IPC) timeout.</p> <p>Workaround: Avoid commands that can cause heavy ethernet traffic on the midplane such as continuous pings or executing the <b>show tech</b> command on MC520H card through a Telnet session.</p> <p>Further Problem Description: The ethernet interrupt will be temporarily disabled under heavy load to give other processes a chance to run. By design, the interrupt should be re-enabled after a short period of time (when a timer expires) or the scheduler finds no processes are ready. The timer is not working on the MC520H card. As a result, the interrupt is disabled for a long time under heavy process load, which in turn causes the IPC timeout.</p>
CSCsj31548	<p>When a U card is replaced with a H card, all Broadcom 3300-based modems have packet loss. This issue is not seen with the U cards.</p> <p>Workaround: Set the preamble length for station and initial IUCs to 100 bits (50 symbols).</p>
CSCsj42426	<p>A Cisco uBR10000 series router can reset unexpectedly.</p> <p>This issue occurs when using Cisco IOS Release 12.3(21a)BC2 and the Dynamic Shared Secret feature.</p> <p>Workaround: Disable the Dynamic Shared Secret feature.</p>
CSCsj52927	<p>DATA CORRUPTION-1-DATA INCONSISTENCY messages appear in the <b>show log</b> output when the router comes up.</p> <p>There are no known workarounds.</p>
CSCsj70948	<p>The PRE2 crashes and then switches over. When removing, inserting, or switching over the line card redundancy, it crashes when removing the last member of HCCP N+1.</p> <p>This issue occurs on a Cisco uBR10000 series router with PRE2 and Global N+1 Redundancy. When perform removing/inserting the global N+1 member and on the other vty, perform <b>show hccp channel</b> at the same time.</p> <p>Workaround: When perform removing/inserting the hccp global N+1 member:</p> <ol style="list-style-type: none"> <li>1. Only remove the global hccp N+1 member on the same VTY.</li> <li>2. Once the member is removed, only perform the command "show hccp brief" until the hccp is normalized. for example, no more counters count down from the "show hccp brief" screen</li> <li>3. Wait for 90 seconds, then, it's safe to perform show hccp channel-switch command.</li> </ol> <p>The key is to wait for the HCCP to complete its database. This is rare occurs, but caution should be taken.</p>

**Table 52**      **Resolved Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsj79192	<p>Moving modems using Dynamic Channel Change (DCC) <b>init tech &gt;=1</b> between two upstream channels causes a line card crash when the following configuration exists for the upstream channels in a cable interface:</p> <pre data-bbox="613 426 1193 478">cable upstream 0 scheduling type ugs mode llq cable upstream 1 scheduling type ugs mode llq</pre> <p>This issue can occur when the CMTS is configured for load balance or some general DCC testing is in progress.</p> <p>Workaround: If you remove the following line from the upstream configuration, the LC crash will not occur:</p> <pre data-bbox="613 657 1193 688">cable upstream 0 scheduling type ugs mode llq</pre>
CSCsj85484	<p>A Cisco uBR10000 series (PRE2-RP) router running Cisco IOS Release 12.3(21)BC crashes with tracebacks when issuing several <b>cable intercept</b> commands.</p> <p>There are no known workarounds.</p>

Table 52 Resolved Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)

DDTS ID Number	Description
CSCsj97292	<p>Under rare conditions, a Hot Standby Connection-to-Connection Protocol (HCCP) switchover and revertback can cause all JIBs to shut down, the UP convertor to be disabled, and all modems to drop. This issue is not necessarily a cable modem termination system (CMTS) problem; sometimes it can be triggered by HCCP issues as well.</p> <p>To diagnose this problem:</p> <ol style="list-style-type: none"> <li>1. Enter the <b>show controller</b> <i>x/y/z</i> command. Note that the output will display: “i Disable”.</li> <li>2. Enter the <b>show hccp detail</b> command. Note that the Member Loading output count is not 0.</li> </ol> <p>Workaround: Recover the modems from offline status by performing the following steps:</p> <ol style="list-style-type: none"> <li>1. Remove the protect member.</li> <li>2. Remove the problematic working member.</li> <li>3. Normalize the new standalone card and get the modems back online. (Note that after the modems are back online, the hccp count value will still be greater than 0 5.)</li> <li>4. Decide whether you want to add the working and protect members back.</li> <li>5. Schedule a maintenance window to recover the hccp Member Loading non 0 count 1.</li> </ol> <p>Recover the hccp Member Loading non 0 count 1 by performing the following steps:</p> <ol style="list-style-type: none"> <li>1. Reset the secondary PRE to re-synchronize the database.</li> <li>2. Check that the secondary PRE is working.</li> <li>3. Perform a switchover to the PRE.</li> <li>4. Enter the <b>show hccp detail</b> command. The Member Loading output count should be 0 5.</li> <li>5. Perform the CLC switchover now to make sure HCCP works as designed. (This step assumes that you have the line card already put back into the global HCCP configuration.)</li> </ol>
CSCsk03541	<p>When using the cable monitor feature for certain cable interfaces, copies of the map-grant packets are not sent to a WAN interface when used on a per service identifier (SID) basis with the Cablevision configuration/setup.</p> <p>This issue occurs in Cisco IOS Release 12.3(21a)BC and later releases when using the <b>cable monitor outbound interface</b> <i>interface-name</i> <b>sid</b> <i>sid-#</i> <b>packet-type</b> <b>mac type</b> <b>map-grant</b> command.</p> <p>Workaround: Do not use the atdma setting in the cable interface.</p>

**Table 52 Resolved Caveats for Cisco IOS Release 12.3(17b)BC9 (continued)**

DDTS ID Number	Description
CSCsk24544	<p>Multiple CPUHOG tracebacks are reported by the HCCP_CTRL process on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17b)BC4, leading to the following MC520U cable line card crash:</p> <pre data-bbox="613 426 1369 478">%SYS-3-CPUHOG: Task is running for (108068)msecs, more than (2000)msecs (8932/20),process = HCCP_CTRL</pre> <p>There are no known workarounds.</p>
CSCsk26979	<p>Dynamic Message Integrity Check (DMIC) may run into an infinite loop, essentially becoming a CPUHOG that brings the router to a software-forced crash.</p> <p>This issue occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(17b)BC08 when DMIC is enabled.</p> <p>Workaround: Disable DMIC.</p>
CSCsk46683	<p>The following debug code was added to debug Inter-Process Communication (IPC) timeout problems in customer networks:</p> <ol data-bbox="621 825 1518 1192" style="list-style-type: none"> <li>1. The IPC timeout err code was split into the following specific error codes: ack buf/protocol timeout, rsp timeout, and nack timeout.</li> <li>2. The log error message was added to all the places where msg send returns errors.</li> <li>3. The log error message was added to all the places where msg enqueue fails.</li> <li>4. To debug an rpc timeout, a timestamps field was added in the cr10k request messages, and a check of the time elapsed at different points along the RPC message route was added.</li> <li>5. Enhancements were added to all the IPC timeout-related error messages to display more info, including cpu usage and KA msgs tx/rx timestamps.</li> </ol>
CSCsj47516	<p>A Cisco uBR10000 series router stops generating fast hello packets intermittently, causing the connected remote router to report its neighbor being down due to “Dead timer expired”.</p> <p>This issue is only seen on a Cisco uBR10000 series router that has more than 20 thousand cable modems online and is seen on PRE1, PRE2, and Cisco IOS Releases 12.3(13a)BC6 and 12.3(17a)BC6:</p> <p>Workaround: Disable fast hellos if CMTS has more than 20, 000 cable modems and use default ospf hello timers instead.</p>

## Open Caveats for Release 12.3(21a)BC3

Table 53 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC3.

**Table 53** Open Caveats for Cisco IOS Release 12.3(21a)BC3

DDTS ID Number	Description
CSCek41611	<p>Cisco uBR10-MC5X20U cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>
CSCek65425	<p>Seven warnings appear in the getnext docsQoSServiceFlowPkts file.</p> <p>There are no known workarounds.</p>
CSCek66377	<p>Not all entries are seen for the Protect line card in the MIB table.</p> <p>There are no known workarounds.</p>
CSCek77615	<p>Sometimes the packets/sec value of the Wideband-Cable interface is incorrect and erratic.</p> <p>There are no known workarounds.</p>
CSCek79167	<p>The 5x20 CLC crashes when a Sunrise Telecom CM-1000 is configured to act as a CM provisioned to do BPI+.</p> <p>This issue is also seen in 12.3(21a)BC2, but not in 12.3(21a)BC1.</p> <p>The following error is seen with debug cable privacy and deb cable bpiapi at the time the BPI auth info packet is received at the CMTS:</p> <pre>Jul 11 15:51:49.714: Root certificate is accepted. Jul 11 15:51:49.718: Success in processing a manufacturer certificate. Jul 11 15:51:49.718: Reading the EURO root cert. Jul 11 15:51:49.746: Failed to open file bootflash:euro-root-cert. Jul 11 15:51:49.746: Failed to open file bootflash:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk0:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk1:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk2:euro-root-cert. Jul 11 15:51:49.746: Failed to open file slot0:euro-root-cert. Jul 11 15:51:49.746: Failed to open file slot1:euro-root-cert.</pre> <p>No euro-cert is install, but root-cert from cable labs is installed on the PRE2's bootflash.</p> <p>There are no known workarounds.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>

**Table 53** Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)

DDTS ID Number	Description
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsg39288	<p>Backup TCC card may experience a reload (IPCOIR-3-TIMEOUT on TCC card).</p> <p>The issue has been experienced on 12.3(9a)BC9, 12.3(13a)BC2 and 12.3(13a)BC6. There are compare errors in the <b>show controllers clock-reference</b> that do increment. However the clocks are not actually drifting apart, even though the errors are incrementing. Because clocks are not actually drifting, redundancy is not affected, except during the brief period when the backup TCC+ card reloads after a IPCOIR timeout.</p> <p>There are no known workarounds.</p>
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre>SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>
CSCsg75417	<p>On an MC520u card, signal-to-noise ratio (SNR) values might drop on an upstream, which could cause modems to drop offline.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC3 with multiple MC520u cards configured for pre-equalization.</p> <p>Workaround: 1. Disable/enable pre-equalization on the upstream. 2. Change the minislot size.</p>
CSCsh19917	<p>Some parent warnings appear when static analysis is performed on the specmib source file.</p> <p>Workaround: No workaround is required. The functionality of the MIB query is not affected.</p>

**Table 53 Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)**

DDTS ID Number	Description
CSCsh38866	<p>When the bundle interface is unconfigured and both the interface and the default interface are shut down at the same time, the interface shows both the active and standby Route Processor (RP) in Inconsistent states.</p> <p>There are no known workarounds.</p>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of “no ip unreachable” under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of “ip unreachable under bundle interface” when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh41508	<p>The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.</p> <p>There are no known workarounds.</p>
CSCsh44794	<p>In the subtract_spectrum_band function, the wrong codes are used to swap the lowband_bound and upper_band.</p> <p>There are no known workarounds.</p>
CSCsh66150	<p>The <b>show cable modem connectivity</b> command output is corrupted under some condition.</p> <p>The following example shows a sample output.</p> <pre> ----- show cable modem connectivity ----- Prim 1st time   Times  %online   Online time           Offline time Sid  online      Online      min   avg   max   min   avg max 9    04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 11   04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 </pre> <p>This issue occurs after PRE switchover.</p> <p>Workaround: Clear cable modem delete.</p>
CSCsh69870	<p>The VTMS algorithm has to be optimized due when CMs with different MIRs are mixed. The Downstream can not be fully utilize by a CM configured with a very high MIR (16-20Mbps), even when there is BW available in such Downstream.</p> <p>There are no known workarounds.</p>

**Table 53**      **Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh70679	When sending a trap due to exceeding a threshold, the admission control system fails to report the correct type of event that triggered the threshold to be exceeded. There are no known workarounds.
CSCsh72746	Intermittent bursts of upstream traffic observed on the outgoing WAN interface. This issue occurs with upstream traffic from RF line cards towards WAN interface. There are no known workarounds.
CSCsh72785	No SNMP trap is generated on behalf of the Redundant PRE state change. This issue may occur on the Redundant PRE configuration and state change of redundant unit. There are no known workarounds.
CSCsh91566	Wideband cable modems becomes offline after CMTS is issued <b>microcode reload pxf</b> . This issue occurs when a CMTS that has cable modems registered as wideband cable modems is issued <b>microcode reload pxf</b> . When this happens, all the wideband cable modems go offline as seen in <b>show cable modem</b> . Workaround: This condition is cleared after the wideband interfaces are issued: shutdown no shutdown
CSCsh95096	On a Cisco uBR10012 running Cisco IOS Release 12.3(21)BC, it is possible to change default connector commands even if modems are online on that upstream connector. There are no known workarounds.
CSCsh96105	Under the following conditions, tracebacks are seen and the modem does not come online. <ul style="list-style-type: none"> <li>• HCCP is configured and activated.</li> <li>• A modem changes upstream to an DOCSIS 2.0 only channel.</li> </ul> Workaround: Delete the modem and let it come online again.
CSCsi09848	Pagent cannot get a predefined IP DHCP pool so it will automatically be assigned the default. (192.168.100.x). This issue occurs when running HA regression cases. Workaround: Rerun the case.
CSCsi20529	When pre-equalization is enabled, modems SNR can drop unexpectedly. It is unknown when this problem may occur. Workaround: Turn off pre-equalizatoin.

Table 53 Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)

DDTS ID Number	Description
CSCsi27520	<p>The following interface RPF configuration commands are accepted on theubr10k even though they are not supported in theubr10k microcode:</p> <pre>ip unicast source reachable-via any allow-default ip unicast source reachable-via rx &lt;1-199&gt; ip unicast source reachable-via rx &lt;1300-2699&gt;</pre> <p>Workaround: Do not configure the unsupported commands.</p>
CSCsi33625	<p>The code automatically changes the acceptable upstream power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This is legal for all US channel width options. BTW, the spelling of dBmV is incorrect as well.</p>
CSCsi41787	<p>The <b>show int if downstream</b> CLI shows “cable interface downstream is up” even though the interface is in shutdown state.</p> <p>There are no known workarounds.</p>
CSCsi48608	<p>ACL configured to the CPE is not available after line card/interface switchover.</p> <p>This issue occurs when using <b>cable {modem   host   device} access-group acl</b>.</p> <p>Workaround: Reconfigure ACL to the CPE manually after switchover.</p>
CSCsi72158	<p>The router may experience a possible Maxim NVRAM problem.</p> <p>This issue may occur on Cisco battery backup NVRAM modules, due to high rates of SER (single and multi-bit Soft Error Rate) and SEL (Single Event Latchup) failures, which are induced by Cosmic Radiation.</p> <p>There are no known workarounds.</p>
CSCsi73342	<p>The host entries are lost after PRE switchover when cli per-dev-acl configured, and any ACL is applied to the host.</p> <p>There are no known workarounds.</p>
CSCsi74026	<p>Multicast traffic that matches MQOS configuration is not forwarded.</p> <p>This condition exists if there is a reload of the PXF while the MQOS configuration is in place.</p> <p>There are no known workarounds.</p>

**Table 53**      **Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)**

DDTS ID Number	Description
CSCsi81513	<p>HCCP status shows that everything is synced and the Protect is ready for switchover, even though nothing has been synced over and the interdb on the Protect LC is empty.</p> <p>A LC switchover after this is totally broken and modems will never register on the Protect LC</p> <p>This happens only when the Blaze FPGA image is changed for the Modena and is being reprogrammed on CMTS bootup.</p> <p>Workaround: The modems will not register on the modular interface when Blaze FPGA is being reprogrammed. As soon as the Blaze is reprogrammed, reload the CMTS as the modems are already down.</p> <p>On reload everything should work correctly.</p>
CSCsi83966	<p>Multiple tracebacks are observed:</p> <pre>313861: Apr 10 07:16:06.784 UTC: %REQGRP-3-SYSCALL: System call for command 72 (slot4/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 6069F510 606B35B0 60C5A09C 60C5B7E0 60C58980 61005A70 610093CC 60FF9910 6101FE0C 60916AC4 60916AA8</pre> <pre>314045: Apr 10 08:16:39.940 UTC: %REQGRP-3-SYSCALL: System call for command 42 (slot4/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 6069F510 606AC4A8 606AEED4 60C898A0 60C89B34 60C5AD40 60C5B188 60C5B834 60C58980 61005A70 610093CC 60FF9910 6101FE0C 60916AC4 60916AA8</pre> <pre>313868: Apr 10 07:18:35.833 UTC: %REQGRP-3-SYSCALL: System call for command 47 (slot4/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 6069F510 606B3D0C 606B4930 6069D1EC 6053BEC4 60886370 60897D40 60916AC4 60916AA8</pre> <p>This issue occurs on an UBR7246VXR with MC28U card. BPI and VPN are not configured and no crashinfo is seen on the PRE or line card.</p> <p>Workaround: Reset the affected line card with hardware module stop/start.</p>
CSCsi85054	<p>When dynamic cable modem load balancing is configured between downstream A and downstream B, and downstream B's service flow admission control thresholds are significantly lower than downstream A's. It appears that load balancing still moves modems across to downstream B, even after violating the prescribed Admission control limits.</p> <p>There are no known workarounds.</p>

Table 53 Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)

DDTS ID Number	Description
CSCsi87195	<p>When you configure frequency using SNMP, the range of frequencies accepted is based on the following formula.</p> $\text{min\_us\_freq} = 5000000 + (\text{channel\_width}/2)$ $\text{max\_us\_freq} = 55000000 - (\text{channel\_width}/2)$ <p>Given a frequency configured, when configuring a channel width that cannot accept the frequency configured already, there should be warning message saying that “channel width cannot be configured with the present frequency”.</p> <p>This problem occurs when the frequency you are trying to configure via SNMP is not within the channel width currently configured on the CMTS router.</p> <p>There are no known workarounds.</p>
CSCsi87821	<p>CMs may re-range with pre-equalization enabled.</p> <p>This issue occurs on a uBR10k with IOS 123-17b.BC4 using mc520u cards and pre-equalization enabled.</p> <p>Workaround: Disable pre-equalization.</p>
CSCsi90691	<p>When all the RF channels are removed from a wideband interface, the BW (bandwidth) shows in the command <b>show interface wide x/y/z:n</b> is not correct. It shows the BW of the last channel removed.</p> <p>There are no known workarounds.</p>
CSCsi91217	<p>The CLI command <b>show hardware</b> does not work.</p> <p>This command works for VXR, but it does not work in 12.2SBU05 and 12.3BC.</p> <p>Workaround: The <b>show version</b> command can be used for this purpose</p>
CSCsi91628	<p>After CM reset, SubMgt configuration for that CM is lost.</p> <p>Workaround: Reconfigure the SubMgt parameters.</p>
CSCsi92001	<p>Some packets become stuck in the default queue of the wideband interface and can not be sent out.</p> <p>This issue only occurs when all the RF channels are removed from this wideband interface.</p> <p>There are no known workarounds.</p>
CSCsj10768	<p>MC5x20h-d line card is frequently crashing with following error in crashinfo file:</p> <pre>Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x604F6C98</pre> <p>There are no known workarounds.</p>
CSCsj12497	<p>When the <b>cable per-dev-acl</b> command is configured, the access-list assigned to the host is not available after a PRE switchover.</p> <p>There are no known workarounds.</p>
CSCsj12597	<p>As part of OSSI requirement, dot3StatsCarrierSenseErrors need to incremented when the cable is removed from FE Interface. However, this is not happening.</p> <p>There are no known workarounds.</p>

**Table 53**      **Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)**

DDTS ID Number	Description
CSCsj14502	<p>In certain cases, CMTS does not send intercept packets out in case of cTapStreamIpInterface is set to -1, while other parameters are set correctly in cTapStreamIpTable and snmpwalk show the cTapStreamIpStatus is active.</p> <p>The issue occurs when configuring a cTapStreamIp entry as follows:</p> <pre> cTapStreamIpInterface = -1 cTapStreamIpDestinationAddress = Addr1 cTapStreamIpDestinationLength = 32 cTapStreamIpSourceAddress = Addr2 cTapStreamIpSourceLength = 32 </pre> <p>and Addr1 is directly connected to a cable interface, Addr2 is routed through another interface and the net mask of outgoing interface for destination Addr2 is greater than the one of Addr1.</p> <p>Workaround: Perform one of the following:</p> <p>(1) Directly set the tapping interface's IfIndex, letting cTapStreamIpInterface != -1 and != 0</p> <p>(2) or, Either set cTapStreamIpSourceAddress or cTapStreamIpDestinationAddress to zero, to avoid conflict</p>
CSCsj18695	<p>An Ubr10k router encounters the following error message:</p> <pre> IDT: %PXF_DMA-3-FBB_LINE_CARD: c10k_chk_ipm() rp_over = 1 ipm_over = 0 slot 18 </pre> <p>This issue has been seen to either unexpectedly reload the pxf or cause errors on the router which will lead to the router unexpectedly reloading.</p> <p>This issue has only been observed on an Ubr10k router.</p> <p>There are no known workarounds.</p>
CSCsj30057	<p>The CMTS responds slowly to the CLI until the 520u LC is reset through the CLI.</p> <p>The 520u line card may reset due to the following:</p> <pre> %REQGRP-3-SYSCALL: System call for command 43 (slot6/0) : Nonblocking request failed (Cause: timeout) </pre> <p>This issue occurs on an uBR10k running 12.3(17b)BC4 with 520u.</p> <p>Workaround: Reset the LC through the CLI.</p>
CSCsj31345	<p>The commit of CSCek77620 had already fixed the problem in geo_cable.</p> <p>Part of the diffs of CSCek77620, which is related to the HCCP function, and inter_cm_instance_t should be committed to the DALI throttle branch to fix this problem in DALI.</p> <p>There are no known workarounds.</p>

Table 53 Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)

DDTS ID Number	Description
CSCsj31629	<p>Wrong subslot in OIR Alarms description printed at log. When alarm source is subslot x/1, it prints subslot 0. Example as:</p> <pre>*Jun 15 17:39:06: %UBR10K_ALARM-6-INFO: ASSERT CRITICAL slot 2/1/0 Active Card          \ Removed OIR Alarm - subslot 0</pre> <p>This issue occurs when Real OIR events occurs or the CLI <b>hw-module slot/subslot x/y reset</b> command is executed.</p> <p>There are no known workarounds.</p>
CSCsj42426	<p>A Cisco uBR10000 series can reset unexpectedly.</p> <p>This issue occurs when using Cisco IOS Release 12.3(21a)BC2 and the Dynamic Shared Secret feature.</p> <p>Workaround: Disable the Dynamic Shared Secret feature.</p>
CSCsj43869	<p>The “map-grant” option should not be included in CLI since “map-grant” can not be seen in upstream direction.</p> <p>There are no known workarounds.</p>
CSCsj43929	<p>When using the cable monitor feature, copies of mac packets are not sent to an external sniffer when used on a per mac-address basis.</p> <p>This issue is seen when using “cable monitor interface &lt;interface_name&gt; mac-address &lt;mac_address of CM&gt; packet-type mac” and is seen on IOS 12.3(13a)BCx / 12.3(17a)BCx / 12.3(21a)BCx</p> <p>There are no known workarounds.</p>
CSCsj47516	<p>An ubr10k could stop generating fast hello packets intermittently, causing the connected remote router to report neighbor being down due to “Dead timer expired”.</p> <p>This issue is only seen on a ubr10k that has more than 20 thousand Cable modems online and is seen on PRE1 &amp; PRE2 and IOS images 12.3(13a)BC6 and 12.3(17a)BC6:</p> <pre>ip ospf dead-interval minimal hello-multiplier 4</pre> <p>Workaround: Disable fast hellos if CMTS has more than 20k CMs and use default ospf hello timers instead.</p>
CSCsj54345	<p>Wideband cable modems become offline after CMTS is issued <b>microcode reload pxf</b>.</p> <p>This issue occurs when a CMTS, which has cable modems registered as wideband cable modems, is issued <b>microcode reload pxf</b>. When this happens, all the wideband cable modems go offline as seen in <b>show cable modem</b>.</p> <p>Workaround: This condition is cleared after the wideband interfaces are issued the <b>shutdown</b> command followed by the <b>no shutdown</b> command.</p>
CSCsj55318	<p>Show inventory displays old SN of TCCplus after OIR.</p> <p>This issue occurs on an uBR10k with tccplus and running 12.3(21)BC image or 12.3BC image.</p> <p>There are no known workarounds.</p>

**Table 53**      **Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)**

DDTS ID Number	Description
CSCsj56262	<p>After customer's DHCP server is re-configured to provide new/different IP addresses to CMs and EMTAs, when EMTA is restarted it obtains successfully a new IP address from DHCP server. However, afterwards it is not able to download the configuration file from TFTP server. A ping from any host behind CMTS to EMTA is not working, but a ping from CMTS to EMTA's IP address is working fine.</p> <p>This issue occurs only when <b>cable source-verify</b> is configured under the cable interface.</p> <p>Workaround: Remove <b>cable source-verify</b> from configuration during re-provisioning.</p>
CSCsj57983	<p>The default-phy-burst is wrongly set to 1522, which makes the packets size &gt; 1496 dropped by MODEM.</p> <p>Workaround: Set the default-phy-burst to default value by "no cable default-phy-burst 1522".</p>
CSCsj58093	<p>CPE ping stops after the wideband (WB) switches to the narrowband (NB) mode. This problem occurs when you shut down the WB interface.</p> <p>Workaround: Execute <b>clear arp</b> or <b>clear cable modem</b> commands to clear the ARP entries and then let the cable modem on the NB to come online.</p>
CSCsj63966	<p>PRE2 may reset due to a PXF DMA Error - Input Command Has Sequence Problem.</p> <p>This issue was observed on a uBR10k running 123-13a.BC6.</p> <p>There are no known workarounds.</p>
CSCsj64207	<p>It seems that the total downstream rate applied to Annex A 256QAM downstreams by admission control is only 1543127 bits per second, as opposed to the real rate which is somewhere around 50Mbps.</p> <p>There are no known workarounds.</p>
CSCsj68403	<p>On an ubr10k with a bundle interface configured with "ip flow ingress" and "mpls netflow egress", the netflow table only shows the ingress flows and never the egress.</p> <p>This issue occurs in a ubr10K running 12.3(21)BC. The trigger for the problem is a router reload or pxf reload.</p> <p>Workaround: Un-configure then reconfigure egress netflow after router reload.</p>

Table 53 Open Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)

DDTS ID Number	Description
CSCsj70948	<p>PRE2 crashes and then switchover. When removing, inserting, or swithing over the line card redundancy, it crashes when removing the last member of HCCP N+1.</p> <p>This issue occurs on an uBR10K with PRE2 and Global N+1 Redundancy. When perform removing/inserting the global N+1 member and on the other vty, perform show hccp channel at the same time.</p> <p>Workaround: When perform removing/inserting the hccp global N+1 member:</p> <ol style="list-style-type: none"> <li>1. Only remove the global hccp N+1 member on the same VTY.</li> <li>2. Once the member is removed, only perform the command "show hccp brief" until the hccp is normalized. for example, no more counters count down from the "show hccp brief" screen</li> <li>3. Wait for 90 seconds, then, it's safe to perform show hccp channel-switch command.</li> </ol> <p>The key is to wait for the HCCP to complete its database. This is rare occurs, but caution should be taken.</p>
CSCsj73475	<p>When SPA is shutdown with "hw-module bay 1/0/1 shut", CMs on other SPA are disconnected and connected as narrow-band.</p> <p>This issue is seen when SPA, which has configuration or is connected with CMs, is shutdown.</p> <p>Workaround: Before shutting down SPA, remove all configuration for that.</p>
CSCsj76551	<p>It was observed that the CM transmit levels are dropping +/- 6dB's lower after a undetermined time period when the use of 2 freqs on one connector. The2 US channels are for 2 mac domains:</p> <pre>connector 0 is for US0 of 6/0/0 and US0 of 6/0/4. 6/0/4 U0 is connector 16 by default and a different JIB.</pre> <p>This issue occurs on an uBR10012 running 12.3(13a)BC6 with mc520u with frequency stacking configured on the US.</p> <p>Workaround: Changing the minislots:</p> <pre>From 2 to 4 to 2</pre>
CSCsj77568	<p>After issuing the <b>test cable ucc</b> command many times, the CM becomes stuck at init(rc). However, it is possible to ping to the CM from uBR10k despite the status init(rc).</p> <p>Workaround: Use "clear cable modem &lt;mac-address&gt; delete".</p>

## Resolved Caveats for Release 12.3(21a)BC3

Table 54 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC3.

**Table 54** Resolved Caveats for Cisco IOS Release 12.3(21a)BC3

DDTS ID Number	Description
CSCed95187	RST packets may contain a non-randomized identification value on the IP header.  This issue is observed on a Cisco platform that receives a TCP SYN packet on a non-listening port.  There are no known workarounds.
CSCeh48684	Identification field is always 0 in the tacacs+ packet with SYN flag. The tacacs packet goes from a cat6509 through a FW to the AAA server. The FW construes this as a Fragment Overlap Attack and drops additional new connections.  There are no known workarounds.
CSCek77979	When an US is configured with 6.4mhz channel width, many modems go offline in an N+1 SO.  The issue might be seen less frequently in a 3.2MHz channel configuration.  The issue may not happen in every LC switchover, but it happens sometimes. There has to be a mix of MC520S or MC520U cards with MC520H cards. In this case the H cards was the Protect one in a N+1 solution.  Workaround: Have Linecards with the same type for an N+1 solution.
CSCek78233	Insertion of an “Unknown SFP” into the Modena SPA will sometimes cause the SIP code to crash.  Workaround: Use only Cisco 1000Base-SX and Cisco 1000Base-T SFP's with the SPA.
CSCsb79076	%SYS-3-TIMERNEG errors and tracebacks are observed while making MGCP RSVP calls on a analog (RGW) setups.  This is observed in 12.4(3.9)T1 IOS version.  There are no known workarounds.
CSCse50735	After a cable line card failover, the dynamic Service Flow (SF)-to-Multiprotocol Label Switching (MPLS) virtual private network (VPN) mapping feature no longer works.  There are no known workarounds.
CSCsg17050	The DOCSIS Set-Top Gateway (DSG) interface configuration is not retained when a 5X20S card is replaced with a 5x20U card, and vice versa.  Workaround: Remove the <b>dsg tg</b> configuration from the global configuration, configure it again, and apply the configuration to the interface.

Table 54 Resolved Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)

DDTS ID Number	Description
CSCsh20158	<p>On a Cisco uBR series cable modem termination system (CMTS), if the <b>cable source-verify dhcp</b> function receives a NAK in response to a Dynamic Host Configuration Protocol (DHCP) leasequery, it stops sending any more leasequeries until the system performs a successful DHCP release/renew.</p> <p>This issue could potentially stop a legitimate user from getting connectivity for a short period of time.</p> <p>There are no known workarounds.</p>
CSCsh24533	<p>The router-id for Open Shortest Path First (OSPF) is not getting synchronized in the standby Performance Routing Engine (PRE).</p> <p>Workaround: After PRE switch over, reconfigure a router-id to OSPF.</p>
CSCsh51283	<p>Sfid and Dropped counts are missing after Route Processor Redundancy (RPR) switchover.</p> <p>There are no known workarounds.</p>
CSCsh84040	<p>Multicast traffic (DSG, static multicast with QOS) is not using the DS multicast SF. As a result, the SF counters for that SF do not increment either.</p> <p>This issue occurs when DSG configuration is present or when static multicast configuration is present with MQOS configuration with multiple groups in the same ACL, and DS multicast traffic is started simultaneously on all groups.</p> <p>Workaround: In case of static multicast case mentioned above, the preventive method is to start traffic on one group at a time (rather than starting on all of them at once), which makes sure that traffic from all groups in that ACL goes to the same DS SF.</p>
CSCsh92986	<p>The latency for the <b>RSH</b> command could increase when they are flowing through an FWSM module.</p> <p>The following issue was observed on an FWSM that is running 2.2 software: (1) The long delay was triggered by using either Cisco IOS Release 12.3(13a)BC1 or (2) Release 12.3(17a)BC1 on routers toward which those RSH commands were sent.</p> <p>Workaround: Either bypass the FWSM module or downgrade to Cisco IOS Release 12.3(9a)BC3, which is not affected by this extra delay issue.</p>
CSCsh98114	<p>The <b>cable wideband auto-reset</b> configuration setting has no affect on cards in subslot 1. As a result, wideband capable modems that register as narrow-band modems while the wideband channels are down will not be forced to re-register when the channels come up.</p> <p>Modems connected to WB channels using C5/1/x, C6/1/x, C7/1/x or C8/1/x for their narrow band ports will not re-register as wideband modems if they come online as narrow band modems while the wideband channel is down.</p> <p>Workaround: The modems can be manually reset with the <b>clear cable modem wideband registered reset</b> command.</p>

**Table 54**      **Resolved Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)**

DDTS ID Number	Description
CSCsi20304	<p>When creating one or more streams with same Source &amp; Destination addresses and cTapStreamIpDestinationLength = 0, the first stream gets deleted properly. On deleting the second stream and others thereafter, the "COMMIT_FAILED_ERROR: 1" error is seen, but the stream does get deleted.</p> <p>This issue occurs when creating more than one streams with same Source &amp; Destination addresses and cTapStreamIpDestinationLength = 0 or cTapStreamIpSourceLength = 0 on the same media.</p> <p>There are no known workarounds.</p>
CSCsi24568	<p>Gigabit Ethernet port could go into a CRITICAL alarm state after a PRE failover.</p> <p>This issue occurs with on aubr10k with (PRE1 or PRE2) running IOS 12.3(21)BC when PRE fails over from Active to Standby.</p> <p>Workaround: Reverting back to PRE that was Active prior to the failover, or reloading the CMTS eliminates the critical alarm.</p>
CSCsi68476	<p>After many hours of voice call generated, PRE crashed with no memory.</p> <p>Workaround: Reload the PRE.</p>
CSCsi78162	<p>A router that has the SNA Switch feature enabled may generate several of the following messages along with tracebacks:</p> <pre data-bbox="613 972 1528 1024">%DATACORRUPTION-1-DATAINCONSISTENCY: copy of xx bytes should be xx bytes</pre> <p>This issue is observed on a Cisco router that runs a Cisco IOS software image that contains the fix for caveat CSCsh87705. A list of the affected releases can be found at:</p> <p><a href="http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsh87705">http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&amp;bugId=CSCsh87705</a></p> <p>Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.</p> <p>There are no known workarounds.</p>
CSCsi92682	<p>The following traceback continuously scroll across the console after a LC failover:</p> <pre data-bbox="613 1392 1528 1518">003021: May 16 09:55:50.586: %SYS-2-BADSHARE: Bad refcount in pak_enqueue, ptr=208161D0, count=0 -Traceback= 60766A98 60766FDC 607E0D68 607F2DB0 607C2284 602C9C94 601796A0 6017999C 6017A3F4 6002F44C 6002C3F0 60027E54 60934994 608B6D64</pre> <p>Workaround: Remove <b>cable monitor</b> commands.</p>
CSCsj03260	<p>When using multiple modulation profile for an upstream, a situation can appear where the modem stay completely offline.</p> <p>This issue occurs when swapping from one modulation profile to another. This is currently only seen on MC-5x20H.</p> <p>Workaround: Perform a <b>shut/not shut</b> the upstream or reconfigure another modulation profile on the upstream, then the one the upstream is active with.</p>

**Table 54** *Resolved Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsj06951	<p>Traceback is seen on the terminal.</p> <p>This issue is seen when configuring user-locale and generating a CNF file under telephony-service.</p> <p>There are no known workarounds.</p>
CSCsj13380	<p>Data corruption messages may be displayed, and show isdn active may show incorrect information for calling number on outgoing calls.</p> <p>This problem is inconsistent, and shows up most frequently with the <b>isdn test call</b> command.</p> <p>There are no known workarounds.</p>
CSCsj61399	<p>The 5x20 CLC crashes when a Sunrise Telecom CM-1000 is configured to act as a CM provisioned to do BPI+.</p> <p>This issue is also seen in 12.3(21a)BC2 but not in 12.3(21a)BC1.</p> <p>DDTS filed as a sev 1 because CM-1000 crashes the active CLC causing a failover. If a second attempt is made to connect the CM-1000 to the CMTS, the protect will crash causing complete failure of all MAC domains on the CLC.</p> <p>The following error is seen with debug cable privacy and deb cable bpiapi at the time the BPI auth info packet is received at the CMTS:</p> <pre>Jul 11 15:51:49.714: Root certificate is accepted. Jul 11 15:51:49.718: Success in processing a manufacturer certificate. Jul 11 15:51:49.718: Reading the EURO root cert. Jul 11 15:51:49.746: Failed to open file bootflash:euro-root-cert. Jul 11 15:51:49.746: Failed to open file bootflash:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk0:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk1:euro-root-cert. Jul 11 15:51:49.746: Failed to open file disk2:euro-root-cert. Jul 11 15:51:49.746: Failed to open file slot0:euro-root-cert. Jul 11 15:51:49.746: Failed to open file slot1:euro-root-cert.</pre> <p>No euro-cert is install, but root-cert from cable labs is installed on the PRE2's bootflash.</p> <p>There are no known workarounds.</p>
CSCsj16292	<p>Following an upgrade to 12.2(18)SXF9, the following message may be displayed:</p> <pre>%DATACORRUPTION-1-DATAINCONSISTENCY: copy error -Traceback=</pre> <p>This message may appear as a result of SNMP polling of PAgP variables, but does not appear to be service impacting.</p> <p>There are no known workarounds.</p>
CSCsj18014	<p>A caller ID may be received with extra characters.</p> <p>This issue is observed when caller ID is enabled on both routers and when the station ID and station name are configured on the FXS side.</p> <p>There are no known workarounds.</p>

**Table 54** *Resolved Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsj18516	<p>CMTS does not allow more than 8 downstream service flows with PHS enabled for a single modem.</p> <p>There are no known workarounds.</p>
CSCsj24738	<p>5x20H: Large timestamp jump from utility card causes CMs to stay offline.</p> <p>If a 5x20H Line Card detects a mismatch between its internal DOCSIS timestamp and the timestamp on the backplane, it reloads the timestamp into the JIB but not the MAP FPGA. If the mismatch is large, the DS/US will be out of sync and modems will not be able to come online.</p> <p>Workaround: Reset the 5x20H line card or OIR the utility card.</p>
CSCsj31548	<p>When a U card is replaced with a H card, all Broadcom 3300 based modem have packet loss. This issue is not seen with the U cards.</p> <p>This issue occurs when a U card is replaced with a H card.</p> <p>Workaround: Set the preamble length for station and initial IUCs to 100 bits (50 symbols).</p>
CSCsj32370	<p>Cable filter group match statistics is not correct at both upstream &amp; downstream.</p> <p>There are no known workarounds.</p>
CSCsj43155	<p>Existing Fragment-Force code allows a threshold and a divisor called the ff_number. The divisor evenly grants fragments once a requests is larger then the threshold.</p> <p>This method of fragmentation makes it difficult to choose the correct threshold and divisor given different modem max-burst.</p> <p>As the max-burst increases, the existing implementation forces the divisor to be greater because we do not want to exceed the CMTS phy-max-burst. This creates excessive fragments which is inefficient.</p> <p>Large CM max-burst (typically used when concatenating multiple pkts).</p> <p>There are no known workarounds.</p>
CSCsj58898	<p>The PCMM policy server polls the ifStackTable (1.3.6.1.2.1.31.1.2) on CMTSs to identify bundle interfaces.</p> <p>In some cases, the following mibs contain wrong/missing informations:</p> <pre>ifStackHigherLayer (1.3.6.1.2.1.31.1.2.1.1) ifStackLowerLayer (1.3.6.1.2.1.31.1.2.1.2) : &lt;/B&gt;</pre> <p>There are no known workarounds.</p>
CSCsi79998	<p>Even though the Cable Modem was provisioned as 1.0, users can not change the qos profile of CM and had an error message.</p> <p>This issue occurs inubr10k running 12.3(21)BC.</p> <p>Workaround: Execute the <b>clear cable modem &lt;CM-MAC-address&gt; delete</b> command.</p>

**Table 54** Resolved Caveats for Cisco IOS Release 12.3(21a)BC3 (continued)

DDTS ID Number	Description
CSCsj20998	The crashinfo file of the UBR10000 may be incomplete. Extra information that is used for debugging unexpected reloads may not be included in the crashinfo file. There are no known workarounds.
CSCsj30106	ifOutUcastPkts does not increment on WB interfaces. There are no known workarounds.
CSCsj36054	The link LED on HH-1GE(uBR10k) remains green despite issuing the <b>shutdown</b> command. The link LED also remains green despite disconnecting the fiber cable. These issues are seen on a 12.3(13a)BC6, 12.3(21a)BC1 or 12.3(21a)BC2 with PRE2(uBR10K) with a Half-Height Gigabit Ethernet Line Card on slot3/0 or 4/0. There are no known workarounds.

## Open Caveats for Release 12.3(21a)BC2

Table 55 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC2.

**Table 55** Open Caveats for Cisco IOS Release 12.3(21a)BC2

DDTS ID Number	Description
CSCek41611	Cisco uBR10-MC5X20U cards may experience a silent reload. This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2. There are no known workarounds.
CSCek64423	The cable line card may power up again when a <b>cable power off</b> command is issued. There are no known workarounds.
CSCek66377	Not all entries are seen for the Protect line card in the MIB table. There are no known workarounds.
CSCek77484	After PRE switchover, hccp sync timers may be in a loop for a long time. There are no known workarounds.
CSCek77487	WB modems may go offline and come back during a pre failover. Workaround: Configure <b>no logging console</b> at the CMTS to avoid WB CM going offline or configure <b>logging rate-limit console all ?</b>
CSCsc20266	Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online. This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems. There are no known workarounds.

**Table 55**      **Open Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCse69641	<p>When the <b>show cable modem s t</b> command is issued soon after a <b>clear cable modem all delete</b> command, the console and vty get stuck.</p> <p>The issue occurs in large-scale environments with more than 5000 modems.</p> <p>Workaround: Do not use the <b>clear cable modem all delete</b> command; delete specific modems instead.</p>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>
CSCsg08747	<p>When IPsec is enabled on the cable modem termination system (CMTS) network interface, but not enabled on the associated PC, a ping from the PC to the CMTS gets an unexpected response.</p> <p>This issue occurs because the security association is enabled on one side and not the other. The expected behavior would be that a ping should fail, but the CMTS replies</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsg17050	<p>The DOCSIS Set-Top Gateway (DSG) interface configuration is not retained when a 5X20S card is replaced with a 5x20U card, and vice versa.</p> <p>Workaround: Remove the <b>dsg tg</b> configuration from the global configuration, configure it again, and apply the configuration to the interface.</p>

Table 55 Open Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)

DDTS ID Number	Description
CSCsg44938	<p>On a Cisco uBR10000 series router running an interface-level Hot Standby Connection-to-Connection Protocol (HCCP) configuration, a swap between the MC520H card and MC520u card forces the first JIB's downstreams into the shutdown state. For instance, if you downgrade from the MC520H card to the MC520u card, notice that the MC520u card shut down Cx/y/0 and Cx/y/2 during the building of its configuration.</p> <p>This issue occurs when the Cisco uBR10000 series router is running Cisco IOS Release 12.3(17a)BC2 with an HCCP Interface-Level configuration and <b>cr10k card slot/subslot oir-compatibility</b> is enabled.</p> <p>Workaround: 1. Enter <b>no shut</b> on the affected interfaces before doing an HCCP revertback, or 2. Remove the interface-level HCCP configuration and replace it with a global HCCP configuration.</p>
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre>SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>
CSCsg75417	<p>On an MC520u card, signal-to-noise ratio (SNR) values might drop on an upstream, which could cause modems to drop offline.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC3 with multiple MC520u cards configured for pre-equalization.</p> <p>Workaround: 1. Disable/enable pre-equalization on the upstream. 2. Change the minislot size.</p>
CSCsh19917	<p>Some parent warnings appear when static analysis is performed on the specmib source file.</p> <p>Workaround: No workaround is required. The functionality of the MIB query is not affected.</p>
CSCsh20158	<p>On a Cisco uBR series cable modem termination system (CMTS), if the <b>cable source-verify dhcp</b> function receives a NAK in response to a Dynamic Host Configuration Protocol (DHCP) leasequery, it stops sending any more leasequeries until the system performs a successful DHCP release/renew.</p> <p>This issue could potentially stop a legitimate user from getting connectivity for a short period of time.</p> <p>There are no known workarounds.</p>
CSCsh24533	<p>The router-id for Open Shortest Path First (OSPF) is not getting synchronized in the standby Performance Routing Engine (PRE).</p> <p>Workaround: After PRE switch over, reconfigure a router-id to OSPF.</p>

**Table 55** *Open Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of “no ip unreachable” under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of “ip unreachable under bundle interface” when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh40309	<p>The burst is not being displayed during a modem upstream (US) trace with Cisco Broadband Troubleshooter (CBT) Version 3.2 when pre-equalization is configured on the US port.</p> <p>This issue occurs only on the 5x20S and U cards when pre-equalization (equalization-coefficient) is configured.</p> <p>This issue doesn't seem to occur on the 28U cards, so it may not be prevalent on the 5x20H either because that card also uses Broadcom for the upstream (US) chip. The TI4522 chip is used on the 5x20S and U cards.</p> <p>Workaround: Do not configure the pre-equalization feature. Note that this feature is off by default.</p>
CSCsh41508	<p>The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.</p> <p>There are no known workarounds.</p>
CSCsh51283	<p>Sfid and Dropped counts are missing after Route Processor Redundancy (RPR) switchover.</p> <p>There are no known workarounds.</p>
CSCsh51877	<p>Fewer than 5% of modems go offline after multiple switchovers triggered by cable power off or test crash command.</p> <p>This issue is observed in the pre_fcs 12.3(21)BC image.</p> <p>There are no known workarounds.</p>
CSCsh52061	<p>After multiple LC switchovers from Working to Protect and reverse using Testcrash w or W cmds, many or all calls drop.</p> <p>There are no known workarounds.</p>

**Table 55 Open Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)**

DDTS ID Number	Description
CSCsh66150	<p>The <b>show cable modem connectivity</b> command output is corrupted under some condition.</p> <p>The following example shows a sample output.</p> <pre> ----- show cable modem connectivity ----- Prim 1st time    Times  %online    Online time          Offline time Sid  online      Online      min    avg    max    min    avg max 9    04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 11   04:45:02    1    100.00  00:00  49710d6h49710d6h00:00  00:00 00:00                     </pre> <p>This issue occurs after PRE switchover.</p> <p>Workaround: Clear cable modem delete.</p>
CSCsh72746	<p>Intermittent bursts of upstream traffic observed on the outgoing WAN interface.</p> <p>This issue occurs with upstream traffic from RF line cards towards WAN interface.</p> <p>There are no known workarounds.</p>
CSCsh72785	<p>No SNMP trap is generated on behalf of the Redundant PRE state change.</p> <p>This issue may occur on the Redundant PRE configuration and state change of redundant unit.</p> <p>There are no known workarounds.</p>
CSCsh91566	<p>Wideband cable modems becomes offline after CMTS is issued <b>microcode reload pxf</b>.</p> <p>This issue occurs when a CMTS that has cable modems registered as wideband cable modems is issued <b>microcode reload pxf</b>. When this happens, all the wideband cable modems go offline as seen in <b>show cable modem</b>.</p> <p>Workaround: This condition is cleared after the wideband interfaces are issued:</p> <pre> shutdown no shutdown                     </pre>
CSCsh95096	<p>On a Cisco uBR10012 running Cisco IOS Release 12.3(21)BC, it is possible to change default connector commands even if modems are online on that upstream connector.</p> <p>There are no known workarounds.</p>
CSCsh96105	<p>Under the following conditions, tracebacks are seen and the modem does not come online.</p> <ul style="list-style-type: none"> <li>• HCCP is configured and activated.</li> <li>• A modem changes upstream to an DOCSIS 2.0 only channel.</li> </ul> <p>Workaround: Delete the modem and let it come online again.</p>

**Table 55**      **Open Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)**

DDTS ID Number	Description
CSCsh98114	<p>The <b>cable wideband auto-reset</b> configuration setting has no affect on cards in subslot 1. As a result, wideband capable modems that register as narrow-band modems while the wideband channels are down will not be forced to re-register when the channels come up.</p> <p>Modems connected to WB channels using C5/1/x, C6/1/x, C7/1/x or C8/1/x for their narrow band ports will not re-register as wideband modems if they come online as narrow band modems while the wideband channel is down.</p> <p>Workaround: The modems can be manually reset with the <b>clear cable modem wideband registered reset</b> command.</p>
CSCsi10153	<p>On a UBR10k, running 12.3(17a)BC2, traffic which is directed to a GRE tunnel is not correctly fragmented. The first packet is send correctly, but the second half of the packet seems to be dropped.</p> <p>There are no known workarounds.</p>
CSCsi20529	<p>When pre-equalization is enabled, modems SNR can drop unexpectedly.</p> <p>It is unknown when this problem may occur.</p> <p>Workaround: Turn off pre-equalization.</p>
CSCsi24568	<p>Gigabit Ethernet port could go into a CRITICAL alarm state after a PRE failover.</p> <p>This issue occurs with on aubr10k with (PRE1 or PRE2) running IOS 12.3(21)BC when PRE fails over from Active to Standby.</p> <p>Workaround: Reverting back to PRE that was Active prior to the failover, or reloading the CMTS eliminates the critical alarm.</p>
CSCsi27161	<p>Aubr10k may experience a PXF reload and the routing protocols will go down for 5-10 seconds; but the Cable modems will stay online.</p> <p>This issue occurs on aubr10k running 12.3(17b)BC3.</p> <p>There are no known workarounds.</p>
CSCsi74026	<p>Multicast traffic that matches MQOS configuration is not forwarded.</p> <p>This condition exists if there is a reload of the PXF while the MQOS configuration is in place.</p> <p>There are no known workarounds.</p>
CSCsi27520	<p>The following interface RPF configuration commands are accepted on theubr10k even though they are not supported in theubr10k microcode:</p> <pre>ip unicast source reachable-via any allow-default ip unicast source reachable-via rx &lt;1-199&gt; ip unicast source reachable-via rx &lt;1300-2699&gt;</pre> <p>Workaround: Do not configure the unsupported commands.</p>

Table 55 Open Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)

DDTS ID Number	Description
CSCsi33625	<p>The code automatically changes the acceptable upstream power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This is legal for all US channel width options. BTW, the spelling of dBmV is incorrect as well.</p>
CSCsi41966	<p>The UBR10000 may generate the following message:</p> <pre>UBR10000-6-BADIPASSIGNMENT: DHCP OFFER dropped : Interface Cablex/y/z Mac abcd.efgh.ijkl SID 2205 L3_Interface Cablex/y/z IP x.y.z.t already assigned to MAC=mnop.qrst.uvwx Interface Cablex/y/z SID 6367</pre> <p>The cable modem may be stuck in init(d) for some hours before coming online.</p> <p>This issue occurs on a CMTS running 12.3(17b)BC3.</p> <p>The Cable Modems are provisioned by an external DHCP server.</p> <p>Workaround: If it is not possible to wait for the CM to come up, then a cable card reset will fix the issue.</p>
CSCsi72158	<p>The router may experience a possible Maxim NVRAM problem.</p> <p>This issue may occur on Cisco battery backup NVRAM modules, due to high rates of SER (single and multi-bit Soft Error Rate) and SEL (Single Event Latchup) failures, which are induced by Cosmic Radiation.</p> <p>There are no known workarounds.</p>
CSCsi73342	<p>The host entries are lost after PRE switchover when cli per-dev-acl configured, and any ACL is applied to the host.</p> <p>There are no known workarounds.</p>
CSCsi79998	<p>Even though the Cable Modem was provisioned as 1.0, users can not change the qos profile of CM and had an error message.</p> <p>This issue occurs inubr10k running 12.3(21)BC.</p> <p>Workaround: Execute the <b>clear cable modem &lt;CM-MAC-address&gt; delete</b> command.</p>

**Table 55**      **Open Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)**

DDTS ID Number	Description
CSCsi81513	<p>HCCP status shows that everything is synced and the Protect is ready for switchover, even though nothing has been synced over and the interdb on the Protect LC is empty.</p> <p>A LC switchover after this is totally broken and modems will never register on the Protect LC</p> <p>This happens only when the Blaze FPGA image is changed for the Modena and is being reprogrammed on CMTS bootup.</p> <p>Workaround: The modems will not register on the modular interface when Blaze FPGA is being reprogrammed. As soon as the Blaze is reprogrammed, reload the CMTS as the modems are already down.</p> <p>On reload everything should work correctly.</p>
CSCsi87821	<p>CMs may re-range with pre-equalization enabled.</p> <p>This issue occurs on a uBR10k with IOS 123-17b.BC4 using mc520u cards and pre-equalization enabled.</p> <p>Workaround: Disable pre-equalization.</p>
CSCsj03260	<p>When using multiple modulation profile for an upstream, a situation can appear where the modem stay completely offline.</p> <p>This issue occurs when swapping from one modulation profile to another. This is currently only seen on MC-5x20H.</p> <p>Workaround: Perform a <b>shut/not shut</b> the upstream or reconfigure another modulation profile on the upstream, then the one the upstream is active with.</p>
CSCsi03598	<p>PRE 2 unexpectedly reloads and goes into a loop.</p> <p>This issue occurs when removing the existing flash card from slot1 of PRE2 and inserting another card and performing a dir all.</p> <p>Workaround: Remove the flash card.</p>
CSCsi09848	<p>Pagent cannot get a predefined IP DHCP pool so it will automatically be assigned the default. (192.168.100.x).</p> <p>This issue occurs when running HA regression cases.</p> <p>Workaround: Rerun the case.</p>

## Resolved Caveats for Release 12.3(21a)BC2

Table 56 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC2.

**Table 56** Resolved Caveats for Cisco IOS Release 12.3(21a)BC2

DDTS ID Number	Description
CSCeg62070	<p>Tracebacks or unexpected reloads are seen during a HTTP transactions with long URLs.</p> <p>The unexpected reload is seen when the length of any token in the URL of the request is excessively long.</p> <p>Workaround: Disable HTTP server using the <b>no ip http server</b> command.</p>
CSCek21720	<p>Tracebacks are seen with packet intercepts during line card (LC) switchover.</p> <p>This issue may occur when LC switchover is performed or while PC calls and class features are in progress.</p> <p>There are no know workarounds.</p>
CSCsb78975	<p>The output of <b>show cable modem connectivity</b> display huge value as followings;</p> <pre> Prim 1st time    Times %online    Online time           Offline time Sid  online      Online      min    avg    max    min    avg max 9    04:45:02    1          100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 11   04:45:02    1          100.00  00:00  49710d6h49710d6h00:00  00:00 00:00                     </pre> <p>This issue may occur during PRE-switchover.</p> <p>There are no known workarounds.</p>
CSCsd67236	<p>A policy-based routing (PBR) map with a set clause does not act on matching packets.</p> <p>This issue occurs on PRE1s on Cisco uBR10000 series routers only.</p> <p>There are no known workarounds.</p>

**Table 56**      **Resolved Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)**

DDTS ID Number	Description
CSCse56501	<p>A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.</p> <p>Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6</a></p>
CSCsg40567	<p>Malformed SSL packets may cause a router to leak multiple memory blocks.</p> <p>This issue is observed on a Cisco router that has the <b>ip http secure server</b> command enabled.</p> <p>Workaround: Disable the <b>ip http secure server</b> command.</p>
CSCsg97718	<p>A QOS profile in use may be allowed to be destroy after a Linecard switchover.</p> <p>This issue is observed on the QOS profile created via CLI or SNMP and enforced to the modems. After a line card switchover these in use profiles (created via CLI or SNMP) is allowed to be destroy.</p> <p>There are no known workarounds.</p>
CSCsh05436	<p>Service flows are refused because downstream latency cannot be met by the card.</p> <p>This issue occurs on interfaces having a negative value in the worst case latency for low latency queue, and is caused by using a noncompliant packetcable setup with the packetcable vanilla command. The <b>packetcable authorize vanilla-docsis-mta</b> command allows the receipt of non-compliant service flows. The issue does not occur in a compliant packetcable setup because the “Downstream Latency” value is not permitted.</p> <p>Workaround: Reset the card.</p>
CSCsh39797	<p>Multicast traffic stops on all modems when acl is configured on a secondary wideband channel. The traffic resumes on all modems after the next igmp query interval.</p> <p>There are no known workarounds.</p>
CSCsh40400	<p>Lower throughput rates occur when the default upstream (US) setting of “token bucket rate limiting with shaping” is enabled.</p> <p>This issue seems to occur because the shaping is causing the rate limiting to kick in too early, resulting in premature delayed grants, and reduced bandwidth.</p> <p>Workaround: Disable shaping and only use token bucket rate limiting if you want to achieve high throughputs in the US.</p>

Table 56 Resolved Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)

DDTS ID Number	Description
CSCsh47765	<p>The <b>show hccp brief</b> command may display the same line endlessly under certain combinations of N+1 switchovers.</p> <p>This issue may occur with continuous switchovers in the following sequence:</p> <ol style="list-style-type: none"> <li>1. Switch from W1-&gt;P using “cable power off &lt;W1&gt;” and then power on W1.</li> <li>2. Wait for sync to finish, then switch back to W1 by using power off and turn the power back on.</li> <li>3. Execute the above two steps for W2 LC switch over too.</li> </ol> <p>To resolve this issue, use “cntrlShift 6” and then powering on the W card.</p> <p>There are no known workarounds.</p>
CSCsh61971	<p>The following error message may be observed on the secondary RP console:</p> <pre>.Feb 20 13:27:28.709: %UBR10000-3-DOCSIS_SYNC_SF: cminstp is NULL: Int Cable5/0/2 MAC 0000.cadd.6caf SFlow prim_sid 12, sid 35, sfid 61, state 1 action CHANGE dir 0.</pre> <p>If an RP switchover event occurs, the modem with MAC address mentioned in this error message may be lost and may need to be reconstructed on the new primary RP.</p> <p>On a UBR10K, when the secondary RP is booted up, the database of DOCSIS Cable Modems is synchronized over to the secondary RP. Due to a race condition between bulksync process and dynamic sync process for a modem, it is possible that the information for this modem is never sent across to the secondary RP when it is booted. This error message is seen when further updates for this modem are sent to the secondary RP.</p> <p>Workaround: After RP switchover occurs, rebuild this modem database using CLI <b>clear cable modem &lt;mac-address&gt; delete</b>.</p>
CSCsh63767	<p>If a downstream service flow with zero maximum sustained rate, zero minimum reserved rate and a non zero maximum downstream latency is created on a uBR10k, then the uBR10k will drop all but the first few packets associated with the service flow.</p> <p>This type of service flow is not DOCSIS compliant. However, some third party equipment tends to create these types of service flows when using non Packetcable VoIP.</p> <p>There are no known workarounds.</p>
CSCsh75026	<p>On the uBR10000, it is not possible to set the trust point of the manufacturer CA certificates using the CLI.</p> <p>At any time, it is not possible to set a manufacturer CA certificate to Trusted or Untrusted using the configuration.</p> <p>Workaround: As required by DOCSIS, setting the trust point is supported only using SNMP.</p>
CSCsh76002	<p>Service flows failed to get admitted or activated.</p> <p>There are no known workarounds.</p>

**Table 56** *Resolved Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh81152	<p>A Cisco uBR7200 or uBR10000 series CMTS does not allow setting the trust state of the Manufacturer CA certificates via CLI.</p> <p>Setting a Manufacturer CA certificate to untrusted does have any effect. A Manufacturer CA certificate cannot be added to the hotlist, which prevents the operator from being able to prevent a specific manufacturer from registering on the network.</p> <p>Workaround: Use SNMP to set the Manufacturer CA to untrusted.</p>
CSCsh96715	<p>The “cable service flow activity-timeout 0” does not appear in running configuration when using a value of 0 (= never timeout). This line does not get displayed in the running configuration even though all non-default configs should get displayed in the running configuration.</p> <p>There are no known workarounds.</p>
CSCsi01470	<p>A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.</p> <p>Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.</p> <p>This advisory is posted at <a href="http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-mvpn.html">http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-mvpn.html</a></p>
CSCsi05020	<p>Ubr10k with a bundle interface configured with <b>ip flow ingress</b> and <b>mpls netflow egress</b>. The netflow table only shows the ingress flows, and never the egress.</p> <p>This issue occurs in aubr10K running 12.3(21)BC, but does not occur in aubr7206VXR running the same IOS and same configuration.</p> <p>There are no known workarounds.</p>
CSCsi07120	<p>Long ping times up to 1000 ms and spurious memory access while investigating latency problem occurs.</p> <p>There are no known workarounds.</p>
CSCsi14917	<p>The cable interface falls into Minor alarm due to Physical Port Link Down [0].</p> <p>This issue occurs during PRE switch over.</p> <p>Workaround: Use <b>shut / no shut</b> on the cable interfaces.</p>

**Table 56 Resolved Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)**

DDTS ID Number	Description
CSCsi22189	<p>Theubr10000/PRE2 reported several RP and PXF unexpectedly reloads.</p> <p>The RP reported message:</p> <pre>%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 74BD35C0 data 74BD40E8 chunkmagic 15A3C78B chunk_freemagic 21CD -Process= "Check heaps", ipl= 0, pid= 5 -Traceback= 6066FEB0 60670054 6067F120</pre> <p>While the PXF unexpected reloads with the message:</p> <pre>Feb 27 20:29:20.785: %UBR10000-6-BADIPSOURCE_BUNDLE: Interface Cable7/0/3, IP packet from invalid source. IP=89.216.182.46, MAC=0018.f85a.7095, Expected Interface=Cable7/0/1 SID=455, Actual Interface=Cable7/0/3 SID=755</pre> <pre>=== Start of Toaster Crashinfo Collection (20:29:21 CET Tue Feb 27 2007) === PXF DMA OQC at End of Descriptor With Non-Zero Continuation Bit</pre> <p>There are no known workarounds.</p>
CSCsi22441	<p>The following error was seen on CMTS when DSC refresh:</p> <pre>*Feb 28 15:30:40.013: %UBR10000-4-DSC_PERMANENT_ADMINISTRATIVE: &lt;133&gt;CMTS[DOCSIS]:&lt;83000203&gt; Service Change rejected - Permanent Administrative. CM Mac Addr &lt;0018.6847.62db&gt; *Feb 28 15:30:40.017: DSx Message TLV received from LC:</pre> <p>This issue is seen when Initiating packetcable calls using SA DPC2203 MTA.</p> <p>Workaround: Set T7 and T8 timers to 0.</p>
CSCsi30772	<p>After upgrade from 12.2BC to 12.3BC, the Packetcable code may start rejecting DSA-Req explicitly containing the poll jitter TLV.</p> <p>Workaround: Either drop the poll jitter altogether or use 12.2BC.</p>
CSCsi50134	<p>On aubr10k running Cisco IOS Release 12.3(17b)BC4, the cable monitor may not generate traffic with a mc520h-d card from some specific interfaces.</p> <p>This issue is seen with ma c520h-d inubr10k, but only in slot 7.</p> <p>There are no known workarounds.</p>

**Table 56** Resolved Caveats for Cisco IOS Release 12.3(21a)BC2 (continued)

DDTS ID Number	Description
CSCsi63490	<p>It appears that after a wideband cable modem is reset, or falls offline and comes back online, the modem's counters appear to be too large for the following commands and equivalent SNMP variables.</p> <pre>show cable modem &lt;modem-mac&gt; qos show cable modem &lt;modem-mac&gt; counters show interface cable &lt;iface-num&gt; service-flow &lt;sfid&gt; qos show interface cable &lt;iface-num&gt; service-flow &lt;sfid&gt; counters</pre> <p>The issue occurs after a cable modem has been reset or falls offline and comes back online. The issue only affects modems in w-online state.</p> <p>The issue only appears to occur when the following global configuration command is configured:</p> <pre>cable primary-sflow-qos11 keep all</pre> <p>Workaround: Have any affected modems deleted with the <b>clear cable modem &lt;mac-address&gt; delete</b> command.</p> <p>Replace the configuration command listed above with <b>cable primary-sflow-qos11 keep snmp-only</b>.</p>
CSCsi67793	<p>Cable ARP Filtering in PXF only reports filtering by service identifier (SID) when issued a command <b>show cable arp-filter</b>.</p> <p>It should display a majority of the “M/S” columns with MAC address and “Pro” field should show “PXF”</p> <p>There are no known workarounds.</p>
CSCsi73848	<p>Secondary PRE (that is standby) onubr10k might crash with a bus error.</p> <p>This issue occurs on aubr10k with a 12.3(21)BC IOS image.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(21a)BC1

Table 57 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC1.

**Table 57** Open Caveats for Cisco IOS Release 12.3(21a)BC1

DDTS ID Number	Description
CSCek66377	<p>Not all entries are seen for the Protect line card in the MIB table.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>

Table 57 Open Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)

DDTS ID Number	Description
CSCsd67236	<p>A policy-based routing (PBR) map with a set clause does not act on matching packets.</p> <p>This issue occurs on PRE1s on Cisco uBR10000 series routers only.</p> <p>There are no known workarounds.</p>
CSCsd92405	<p>A router crashes when receiving multiple malformed Transparent LAN Service (TLS) and/or Secure Socket Layer (SSL) 3 finished messages. A valid username and password are not required for the crash to occur.</p> <p>This issue occurs when a router has an Hypertext Transport Protocol (HTTP) secure server enabled and has an open, unprotected HTTP port.</p> <p>Workaround: There are no known workarounds. You can minimize the chances of the condition occurring by permitting only legitimate hosts to access HTTP on the router.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsh05436	<p>Service flows are refused because downstream latency cannot be met by the card.</p> <p>This issue occurs on interfaces having a negative value in the worst case latency for low latency queue, and is caused by using a noncompliant packetcable setup with the packetcable vanilla command. The <b>packetcable authorize vanilla-docsis-mta</b> command allows the receipt of non-compliant service flows. The issue does not occur in a compliant packetcable setup because the “Downstream Latency” value is not permitted.</p> <p>Workaround: Reset the card.</p>
CSCsh19917	<p>Some parent warnings appear when static analysis is performed on the specmib source file.</p> <p>Workaround: No workaround is required. The functionality of the MIB query is not affected.</p>
CSCsh20158	<p>On a Cisco uBR series cable modem termination system (CMTS), if the <b>cable source-verify dhcp</b> function receives a NAK in response to a Dynamic Host Configuration Protocol (DHCP) leasequery, it stops sending any more leasequeries until the system performs a successful DHCP release/renew.</p> <p>This issue could potentially stop a legitimate user from getting connectivity for a short period of time.</p> <p>There are no known workarounds.</p>
CSCsh24533	<p>The router-id for Open Shortest Path First (OSPF) is not getting synchronized in the standby Performance Routing Engine (PRE).</p> <p>Workaround: After PRE switch over, reconfigure a router-id to OSPF.</p>
CSCsh39797	<p>Multicast traffic stops on all modems when acl is configured on a secondary wideband channel. The traffic resumes on all modems after the next igmp query interval.</p> <p>There are no known workarounds.</p>

**Table 57**      **Open Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh41508	The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.  There are no known workarounds.
CSCsh72785	No SNMP trap is generated on behalf of the Redundant PRE state change.  This issue may occur on the Redundant PRE configuration and state change of redundant unit.  There are no known workarounds.
CSCsh75026	On the uBR10000, it is not possible to set the trust point of the manufacturer CA certificates using the CLI.  At any time, it is not possible to set a manufacturer CA certificate to Trusted or Untrusted using the configuration.  Workaround: As required by DOCSIS, setting the trust point is supported only using SNMP.
CSCsh76002	Service flows failed to get admitted or activated.  There are no known workarounds.
CSCsh96715	The “cable service flow activity-timeout 0” does not appear in running configuration when using a value of 0 (= never timeout). This line does not get displayed in the running configuration even though all non-default configs should get displayed in the running configuration.  There are no known workarounds.
CSCsh47765	The <b>show hccp brief</b> command may display the same line endlessly under certain combinations of N+1 switchovers.  This issue may occur with continuous switchovers in the following sequence: <ol style="list-style-type: none"> <li>1. Switch from W1-&gt;P using “cable power off &lt;W1&gt;” and then power on W1.</li> <li>2. Wait for sync to finish, then switch back to W1 by using power off and turn the power back on.</li> <li>3. Execute the above two steps for W2 LC switch over too.</li> </ol> To resolve this issue, use “cntrlShift 6” and then powering on the W card.  There are no known workarounds.
CSCek21720	Tracebacks are seen with packet intercepts during line card (LC) switchover.  This issue may occur when LC switchover is performed or while PC calls and class features are in progress.  There are no know workarounds.
CSCek41611	Cisco uBR10-MC5X20U cards may experience a silent reload.  This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.  There are no known workarounds.
CSCek64423	The cable line card may power up again when a <b>cable power off</b> command is issued.  There are no known workarounds.

**Table 57** Open Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)

DDTS ID Number	Description
CSCek71992	<p>The MC5x20 line card may unexpectedly reload during HCCP switchover.</p> <p>There are no known workarounds.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>
CSCsc99211	<p>After switchover, some modems go offline and some calls are dropped.</p> <p>This issue occurs after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCsd20606	<p>A parallel express forwarding (PXF) restart disables multicast traffic that matches the Multicast Quality of Service (MQoS) configuration.</p> <p>This issue occurs when an MQoS configuration is applied to cable interfaces, and PXF is restarted.</p> <p>There are no known workarounds.</p>
CSCse69641	<p>When the <b>show cable modem s t</b> command is issued soon after a <b>clear cable modem all delete</b> command, the console and vty get stuck.</p> <p>The issue occurs in large-scale environments with more than 5000 modems.</p> <p>Workaround: Do not use the <b>clear cable modem all delete</b> command; delete specific modems instead.</p>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>
CSCsg08747	<p>When IPSec is enabled on the cable modem termination system (CMTS) network interface, but not enabled on the associated PC, a ping from the PC to the CMTS gets an unexpected response.</p> <p>This issue occurs because the security association is enabled on one side and not the other. The expected behavior would be that a ping should fail, but the CMTS replies.</p> <p>There are no known workarounds.</p>
CSCsg17050	<p>The DOCSIS Set-Top Gateway (DSG) interface configuration is not retained when a 5X20S card is replaced with a 5x20U card, and vice versa.</p> <p>Workaround: Remove the <b>dsg tg</b> configuration from the global configuration, configure it again, and apply the configuration to the interface.</p>

**Table 57**      **Open Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)**

DDTS ID Number	Description
CSCsg44938	<p>On a Cisco uBR10000 series router running an interface-level Hot Standby Connection-to-Connection Protocol (HCCP) configuration, a swap between the MC520H card and MC520u card forces the first JIB's downstreams into the shutdown state. For instance, if you downgrade from the MC520H card to the MC520u card, notice that the MC520u card shut down Cx/y/0 and Cx/y/2 during the building of its configuration.</p> <p>This issue occurs when the Cisco uBR10000 series router is running Cisco IOS Release 12.3(17a)BC2 with an HCCP Interface-Level configuration and <b>cr10k card slot/subslot oir-compatibility</b> is enabled.</p> <p>Workaround: 1. Enter <b>no shut</b> on the affected interfaces before doing an HCCP revertback, or 2. Remove the interface-level HCCP configuration and replace it with a global HCCP configuration.</p>
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre>SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachable" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachable" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh40234	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC6, reports the following message with traceback in the log of the active PRE1 for many different cable modems:</p> <pre>Jan 10 10:29:26 EST: %UBR10000-3-INVALIDSIDPOSITION: Invalid SID (2166) position for interface Cable5/0/0: CM 0011.e358.5d05:Is used by CM 0090.649d.2795 SFID 3679 SID 1834.SID container info: start 8170 end 5766</pre> <p>There are no known workarounds.</p>

**Table 57** *Open Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh40309	<p>The burst is not being displayed during a modem upstream (US) trace with Cisco Broadband Troubleshooter (CBT) Version 3.2 when pre-equalization is configured on the US port.</p> <p>This issue occurs only on the 5x20S and U cards when pre-equalization (equalization-coefficient) is configured.</p> <p>This issue doesn't seem to occur on the 28U cards, so it may not be prevalent on the 5x20H either because that card also uses Broadcom for the upstream (US) chip. The TI4522 chip is used on the 5x20S and U cards.</p> <p>Workaround: Do not configure the pre-equalization feature. Note that this feature is off by default.</p>
CSCsh40400	<p>Lower throughput rates occur when the default upstream (US) setting of "token bucket rate limiting with shaping" is enabled.</p> <p>This issue seems to occur because the shaping is causing the rate limiting to kick in too early, resulting in premature delayed grants, and reduced bandwidth.</p> <p>Workaround: Disable shaping and only use token bucket rate limiting if you want to achieve high throughputs in the US.</p>
CSCsh50221	<p>The MC5x20 line card crashes on a Cisco uBR10000 series router IOS running Cisco IOS Release 12.3(13a)BC6 because of a bus error exception.</p> <p>There are no known workarounds.</p>
CSCsh51283	<p>Sfid and Dropped counts are missing after Route Processor Redundancy (RPR) switchover.</p> <p>There are no known workarounds.</p>
CSCsh51877	<p>Fewer than 5% of modems go offline after multiple switchovers triggered by cable power off or test crash command.</p> <p>This issue is observed in the pre_fcs 12.3(21)BC image.</p> <p>There are no known workarounds.</p>
CSCsh52061	<p>After multiple LC switchovers from Working to Protect and reverse using Testcrash w or W commands, many or all calls drop.</p> <p>There are no known workarounds.</p>
CSCsh54779	<p>Standby Inconsistent messages are seen on Standby RPs.</p> <p>This issue only affects the 12.3(21)BC release, and only occurs on the secondary RP.</p> <p>There are no known workarounds.</p>
CSCsh63767	<p>If a downstream service flow with zero maximum sustained rate, zero minimum reserved rate and a non zero maximum downstream latency is created on a uBR10k, then the uBR10k will drop all but the first few packets associated with the service flow.</p> <p>This type of service flow is not DOCSIS compliant. However, some third party equipment tends to create these types of service flows when using non Packetcable VoIP.</p> <p>There are no known workarounds.</p>

**Table 57**      **Open Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)**

DDTS ID Number	Description
CSCsh70146	<p>On a UBR10K, the syslog message for OVERLAPIP has the potential to be generated and overwhelming amount. This can reduce the visibility of important syslog messages that monitor CMTS health and/or overburden syslog servers.</p> <p>As customers deploy UBR10Ks in their network and ramp up the number of CMs/CPEs on those CMTSs, the frequency of these OVERLAPIP syslog messages jumps.</p> <p>Workaround: Perform a <b>show log   e OVERLAPIP</b>, but this does not help the burden put on syslog servers.</p>
CSCsh70767	<p>The tunnel interface can not forward upstream traffic and returns an error destination unreachable icmp packet from bundle interface. The source ip address of icmp packet is 0.0.0.0</p> <p>This issue occurs on a Cisco ubr10k with pre-1 connected with a router for gre tunnel peer.</p> <p>Workaround: Configure the gre tunnel between the cmts uplink port and router.</p>
CSCsh70869	<p>Intermittently, cable modems are not using the tos value defined in the qos profile.</p> <p>If following is defined in the configuration:</p> <pre>cable qos profile 219 tos-overwrite 0xFF 0x10</pre> <p>We can see the following in the qos output:</p> <pre>cm04cor#sh cab mode 10.1.113.35 ver QoS Profile Index           : 219 IP Type of Service AND-mask      0xFF  &lt;&lt;&lt; IP Type of Service OR-mask      0x10  &lt;&lt;&lt;&lt;</pre> <pre>cm04cor#sh cab mode 10.1.113.35 qos ver Request/Transmission policy      : 0x0  &lt;--- IP ToS Overwrite[AND-mask, OR-mask] : 0x0, 0x0 &lt;---</pre> <p>There are no known workarounds.</p>
CSCsh72746	<p>Intermittent bursts of upstream traffic observed on the outgoing WAN interface.</p> <p>This issue occurs with upstream traffic from RF line cards towards WAN interface.</p> <p>There are no known workarounds.</p>
CSCsh90680	<p>Occasional CMTS-initiated TCP Reset of the connection to the collector. When it occurs, it always occurs close to the end of the exported document and causes loss of remaining flow record information from that export interval.</p> <p>There are no known workarounds.</p>
CSCsh90684	<p>Occasional, there is an incorrect IPDR document header at the beginning of an export. This causes a complete failure of that document export attempt. Typically, the next document export attempt at the next reporting interval succeeds.</p> <p>There are no known workarounds.</p>

Table 57 Open Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)

DDTS ID Number	Description
CSCsh90688	Occasionally, very slow export performance (approximately a factor of 50 slower than normal) occurs.  This issue causes exports to be received at a frequency of only approximately every 4-6 hours instead of the normal period of approximately every 25minutes.  There are no known workarounds.
CSCsh91566	Wideband cable modems becomes offline after CMTS is issued <b>microcode reload pxf</b> .  This issue occurs when a CMTS that has cable modems registered as wideband cable modems is issued <b>microcode reload pxf</b> . When this happens, all the wideband cable modems go offline as seen in <b>show cable modem</b> .  Workaround: This condition is cleared after the wideband interfaces are issued:  shutdown no shutdown
CSCsh95096	On a Cisco uBR10012 running Cisco IOS Release 12.3(21)BC, it is possible to change default connector commands even if modems are online on that upstream connector.  There are no known workarounds.
CSCsh95155	Deleting snmp private RW from 10K still allows RF Switch to Toggle.  This issue occurs when using the RF switch for line card high availability, and the private RW string is removed from the CMTS.  Workaround: Do not delete/remove the private rw snmp string from the CMTS, or be sure to configure the same RW string on the RF S witch(s) and 10K. The HCCP/SNMP string can be changed on the 10K with 12.3(13) code and >.
CSCsh95284	UBR 10000 receives the following error messages without any software or hardware changes.  SLOT 7/0: Feb 22 21:22:33.160: %SYS-2-LINKED: Bad enqueue of 62BA698C in queue 61E65540 -Process= "CMTS MAC Protocol", ipl= 3, pid= 37 -Traceback= 60151B04 60218BC4 602950F0 602290B8 60217354 602125D8 60213168 6030A300  Workaround: According to previous cases, use Cu to reset the module in Slot 7.
CSCsi01137	Gigabit interface on UBR 10K stops forwarding traffic.  Workaround: Reload the router enables back forwarding.
CSCsi03598	PRE 2 unexpectedly reloads and goes into a loop.  This issue occurs when removing the existing flash card from slot1 of PRE2 and inserting another card and performing a dir all.  Workaround: Remove the flash card.

**Table 57**      **Open Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsi05020	Ubr10k with a bundle interface configured with <b>ip flow ingress</b> and <b>mpls netflow egress</b> . The netflow table only shows the ingress flows, and never the egress.  This issue occurs in aubr10K running 12.3(21)BC, but does not occur in aubr7206VXR running the same IOS and same configuration.  There are no known workarounds.
CSCsi07120	Long ping times up to 1000 ms and spurious memory access while investigating latency problem occurs.  There are no known workarounds.
CSCsi09848	Pagent cannot get a predefined IP DHCP pool so it will automatically be assigned the default. (192.168.100.x).  This issue occurs when running HA regression cases.  Workaround: Rerun the case.
CSCsi10153	On a UBR10k, running 12.3(17a)BC2, traffic which is directed to a GRE tunnel is not correctly fragmented. The first packet is send correctly, but the second half of the packet seems to be dropped.  There are no known workarounds.
CSCsi13883	Access-list number from the snmp-server community command in the global config gets removed  This issue is seen when <b>rf-switch snmp community</b> command is added under the redundancy sub-command.  Workaround: To avoid this issue, configure the <b>snmp-server community</b> command after the redundancy rf-switch snmp community sub-command.
CSCsi14917	The cable interface falls into Minor alarm due to Physical Port Link Down [0].  This issue occurs during PRE switch over.  Workaround: Use <b>shut / no shut</b> on the cable interfaces.

## Resolved Caveats for Release 12.3(21a)BC1

Table 58 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21a)BC1.

**Table 58 Resolved Caveats for Cisco IOS Release 12.3(21a)BC1**

<b>DDTS ID Number</b>	<b>Description</b>
CSCei19563	<p>A faulty PRE may unexpectedly switch from standby mode to active mode, causing the active PRE to unexpectedly reload.</p> <p>This issue is observed on a Cisco 10000 series that has dual PREs and runs Cisco IOS Release 12.0(25)SX6, but may also occur in Release 12.0S.</p> <p>Workaround: Remove the faulty PRE.</p>
CSCek65980	<p>The <b>cops listener access-list</b> command disappears from the running configuration after a cable modem termination system (CMTS) reload, however, it stays in startup configuration.</p> <p>Workaround: Issue the <b>cops listener access-list acl-num</b> command after the router boots up.</p>
CSCsd20683	<p>A command switchover with a virtual interface (VI) configuration is not switching the whole line card.</p> <p>By default, when VI is enabled on an interface, the Hot Standby Connection-to-Connection Protocol (HCCP) line card should switchover the whole line card instead of switching an individual domain.</p> <p>There are no known workarounds.</p>
CSCsd30267	<p>The Authentication, Authorization, and Accounting (AAA) per user process is holding memory, and the router is running out of memory.</p> <p>This issue occurs when PPP over Ethernet (PPPoE) dialing and dynamic access control lists (ACLs) are present.</p> <p>There is no known workaround.</p>
CSCsd33394	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), upstream subscriber traffic management filters do not filter packets with a multicast destination IP address.</p> <p>Workaround: Configure and apply an ip access-list to the cable or bundle interface. This configuration will apply to traffic from all modems and CPE on the interface.</p>

**Table 58 Resolved Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)**

DDTS ID Number	Description
CSCsd85587	<p>A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).</p> <p>Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.</p> <p>The vulnerable cryptographic library is used in the following Cisco products:</p> <p>Cisco IOS, documented as Cisco bug ID CSCsd85587</p> <p>Cisco IOS XR, documented as Cisco bug ID CSCsg41084</p> <p>Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999</p> <p>Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348</p> <p>Cisco Firewall Service Module (FWSM)</p> <p>This vulnerability is also being tracked by CERT/CC as VU#754281.</p> <p>Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto</a></p> <hr/> <p> <b>Note</b> Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at <a href="http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml</a> and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL</a></p>
CSCse04894	<p>Setting the lockout flag on the Working line card and then performing a <b>hw-module subslot x/y reset</b> of the line card causes a switchover from the Working to the Protect line card, disables the upconverter on the Active Protect line card, and causes all modems to go offline.</p> <p>There are no known workarounds.</p>

Table 58 Resolved Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)

DDTS ID Number	Description
CSCse05736	<p>A router running RCP can be reloaded by a specific packet.</p> <p>This issue is seen under the following conditions:</p> <ul style="list-style-type: none"> <li>• The router must have RCP enabled.</li> <li>• The packet must come from the source address of the designated system configured to send RCP packets to the router.</li> <li>• The packet must have a specific data content.</li> </ul> <p>Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.</p>
CSCsg39990	<p>Cable filter groups do not filter local traffic on the Cisco uBR10000 series platform.</p> <p>There are no known workarounds.</p>
CSCsg90384	<p>Cable filter-groups do not filter based on type-of-service (ToS) value except when the <b>mask</b> "0x0" and <b>tos</b> "0x0" values are used.</p> <p>The CMTS_PKT_FILTER_GROUP_x access-list built by the filter group always contains the following statement irrespective of the <b>mask</b> and <b>tos</b> values entered under the <b>cable filter-group</b> command except when the <b>mask</b> "0x0" and <b>tos</b> "0x0" values are used:</p> <pre>10K#sh access-list CMTS_PKT_FILTER_GROUP_2 Load for five secs: 5%/2%; one minute: 5%; five minutes: 5% Time source is NTP, 18:38:52.458 PST Wed Nov 29 2006 Extended IP access list CMTS_PKT_FILTER_GROUP_2 (per-user) (Compiled) (PXF security) (snip) deny ip any any precedence routine (snip)</pre> <p>When the <b>mask</b> "0x0" and <b>tos</b> "0x0" values are used, the access-list statement changes to <b>deny ip any any</b>, which is the proper behavior defined by the DOCSIS OSSI specification. Other filter parameters, such <b>src/dest ip</b> or <b>src/dest tcp/udp port #</b>, work correctly.</p> <p>There are no known workarounds.</p>
CSCsh06777	<p>The cable filter group assigned to the cable modem is not applied. Instead, the filter group of the customer premises equipment (CPE) is applied instead.</p> <p>There are no known workarounds.</p>
CSCsh11414	<p>A Cisco UBR10000 series router running Cisco IOS Release 12.3(17a)BC2 and configured for Subscriber Account Management Interface Specification (SAMIS) does not save deleted service flows for an offline cable modem if the <b>cable primary-sflow-qos11 keep all</b> command is configured. Consequently, the deleted service flows are absent from the SAMIS and the docsQosServiceFlowLogTable.</p> <p>Workaround: Remove the <b>cable primary-sflow-qos11 keep all</b> command to save the deleted service flow information.</p>

**Table 58 Resolved Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh29217	<p>Cisco 10000, uBR10012 and uBR7200 series devices use a User Datagram Protocol (UDP) based Inter-Process Communication (IPC) channel that is externally reachable. An attacker could exploit this vulnerability to cause a denial of service (DoS) condition on affected devices. No other platforms are affected.</p> <p>Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc</a></p>
CSCsh30009	<p>A Cisco Router running an IOS version that has contains the bug fix for CSCsg21394 may fail to resolve Canonical Names (CNAME) DNS queries.</p> <pre>Router#ping http://www.google.com  Translating "http://www.google.com"...domain server (x.x.x.x)  Translating "http://www.google.com"...domain server (x.x.x.x) Domain: Using source interface FastEthernet4 Domain: query for http://www.google.com type 1 to x.x.x.x DOM: dom2cache: hostname is http://www.google.com, RR type=5, class=1, ttl=0, n=8 DOM: Answer hostname doesn't match query hostnameReply received empty Domain: query for http://www.google.com.domain.com type 1 to x.x.x.xReply received no such name Domain: Using source interface FastEthernet4 Domain: query for h</pre> <p>There are no known workarounds.</p>
CSCsh73925	<p>A Cisco uBR7200 or uBR10000 series CMTS may lose ip connectivity to CM/CPE devices after removing a secondary IP address on a cable or bundle interface.</p> <p>Removing a secondary ip address causes all ARP entries (associated with primary ip address and remaining secondary ip addresses) on that bundle interface to be deleted. Until the ARP table is rebuilt there could be loss of ip connectivity.</p> <p>Workaround: Ensure that secondary IP addresses are removed during a maintenance window.</p> <p>Another potential workaround would be to segment the CMTS into smaller cable interface bundle groups or to use separate subinterfaces so that a lower number of modems and CPE ARP entries are linked to each subinterface.</p>
CSCsh84786	<p>After a PRE switchover on theubr10k, the data path to the cable line cards may fail due to a race condition in determining the primary PRE. L3 data traffic through the cable line card is dropped.</p> <p>This is a race condition which may happen after a PRE switchover from PRE.</p> <p>Workaround: Reset the affected cable line card.</p>

**Table 58** Resolved Caveats for Cisco IOS Release 12.3(21a)BC1 (continued)

DDTS ID Number	Description
CSCsh86580	<p>When doing a CLC switchover in N+1 configuration mode and the protect line card is 520H card, the CMs on the protect card will be come offline.</p> <p>The CMs will not recover from offline state unless there is human intervention</p> <p>Workaround: There are two ways to recover:</p> <ol style="list-style-type: none"> <li>1. Revert back</li> <li>2. clear interface x/x/x</li> </ol> <p>The following needs to be done for each sub interface.</p> <pre>clear interface cable 5/1/0 clear interface cable 5/1/1 clear interface cable 5/1/2 clear interface cable 5/1/3 clear interface cable 5/1/4</pre>
CSCsi04244	<p>On Cisco UBR10K with two PREs, when default route is configured, traffic should recover after PRE switchover within 2.5 seconds. If static ARP is configured, the traffic may be dropped for up to 6 seconds in the case of static default route and up to 30 seconds with OSPF generated default route.</p> <p>Static ARP is configured for the IP address of next hop WAN router, specified as default gateway in the <b>ip route 0.0.0.0 0.0.0.0 &lt;a.b.c.d&gt;</b> command.</p> <p>Workaround: Remove static ARP and use dynamic ARP for next hop router IP address on WAN side.</p>

## Open Caveats for Release 12.3(21)BC

Table 59 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21)BC.

**Table 59** Open Caveats for Cisco IOS Release 12.3(21)BC

DDTS ID Number	Description
CSCek21720	<p>Tracebacks are seen with packet intercepts during line card (LC) switchover.</p> <p>This issue may occur when LC switchover is performed or while PC calls and class features are in progress.</p> <p>There are no know workarounds.</p>
CSCek41611	<p>Cisco uBR10-MC5X20U cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>

**Table 59** *Open Caveats for Cisco IOS Release 12.3(21)BC (continued)*

DDTS ID Number	Description
CSCek66923	<p>The following changes have been made to the debug code:</p> <ul style="list-style-type: none"> <li>• New debug code has been added to <code>cmts_delete_entry()</code> to catch when any application uses this function and leaves a dangling pointer in the service identifier (SID) <code>host_chains</code>.</li> <li>• The deliberate crash from <code>is_cmts_entry_poisoned()</code> has been removed due to the new debug code added in step 1 above.</li> </ul> <p>There are no known workarounds.</p>
CSCin98031	<p>N+1 sync does not occur when switching over from a Working card to Protect card.</p> <p>There are no known workarounds.</p>
CSCsb86099	<p>While performing a switchover, the following error message occurs. After multiple switchovers, the router unexpectedly crashes:</p> <pre>Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC2 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC3 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC4 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US2 Physical Port Link Down</pre> <p>This issue occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>• Performing a Route Processor Redundancy (RPR) switchover using the CLI.</li> <li>• Performing multiple switchovers</li> </ul> <p>There are no known workarounds</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a <code>REG_REQ</code> that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>

Table 59 Open Caveats for Cisco IOS Release 12.3(21)BC (continued)

DDTS ID Number	Description
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsc99211	<p>After switchover, some modems go offline and some calls are dropped.</p> <p>This issue occurs after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCsd20606	<p>A parallel express forwarding (PXF) restart disables multicast traffic that matches the Multicast Quality of Service (MQoS) configuration.</p> <p>This issue occurs when an MQoS configuration is applied to cable interfaces, and PXF is restarted.</p> <p>There are no known workarounds.</p>
CSCsd20683	<p>A command switchover with a virtual interface (VI) configuration is not switching the whole line card.</p> <p>By default, when VI is enabled on an interface, the Hot Standby Connection-to-Connection Protocol (HCCP) line card should switchover the whole line card instead of switching an individual domain.</p> <p>There are no known workarounds.</p>
CSCsd29450	<p>A Protect line card unexpected reloads after a sequence of route processor (RP) and LC switchovers.</p> <p>This issue occurs when performing a sequence of LC and Performance Routing Engine (PRE) switchovers.</p> <p>There are no known workarounds</p>
CSCsd47667	<p>The cable meter feature is causing redundancy to fail between PRE2s due to Inter-Process Communication (IPC) timeouts.</p> <p>This issue occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC2 or 12.3(17a)BC.</p> <p>Workaround: Reload the standby PRE2.</p>
CSCsd67236	<p>A policy-based routing (PBR) map with a set clause does not act on matching packets.</p> <p>This issue occurs on PRE1s on Cisco uBR10000 series routers only.</p> <p>There are no known workarounds.</p>
CSCsd98200	<p>Spurious memory access occurs while doing a line card switchover.</p> <p>There are no known workarounds.</p>
CSCse69641	<p>When the <b>show cable modem s t</b> command is issued soon after a <b>clear cable modem all delete</b> command, the console and vty get stuck.</p> <p>The issue occurs in large-scale environments with more than 5000 modems.</p> <p>Workaround: Do not use the <b>clear cable modem all delete</b> command; delete specific modems instead.</p>

**Table 59**      **Open Caveats for Cisco IOS Release 12.3(21)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>
CSCsg08747	<p>When IPsec is enabled on the cable modem termination system (CMTS) network interface, but not enabled on the associated PC, a ping from the PC to the CMTS gets an unexpected response.</p> <p>This issue occurs because the security association is enabled on one side and not the other. The expected behavior would be that a ping should fail, but the CMTS replies.</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsg17050	<p>The DOCSIS Set-Top Gateway (DSG) interface configuration is not retained when a 5X20S card is replaced with a 5x20U card, and vice versa.</p> <p>Workaround: Remove the <b>dsg tg</b> configuration from the global configuration, configure it again, and apply the configuration to the interface.</p>
CSCsg41805	<p>A cable modem is not ping-able after a reset modem from the cable modem termination system (CMTS). The cable modem gets stuck in the init(d) state and is not able to come online.</p> <p>This issue occurs in Hot Standby Connection-to-Connection Protocol (HCCP) line card redundancy and virtual interface (VI) bundle interface configurations and can occur on the Protect line card after different line card failovers and Route Processor switchovers.</p> <p>Workaround: Failover back to the Working line card.</p>
CSCsg44938	<p>On a Cisco uBR10000 series router running an interface-level Hot Standby Connection-to-Connection Protocol (HCCP) configuration, a swap between the MC520H card and MC520u card forces the first JIB's downstreams into the shutdown state. For instance, if you downgrade from the MC520H card to the MC520u card, notice that the MC520u card shut down Cx/y/0 and Cx/y/2 during the building of its configuration.</p> <p>This issue occurs when the Cisco uBR10000 series router is running Cisco IOS Release 12.3(17a)BC2 with an HCCP Interface-Level configuration and <b>cr10k card slot/subslot oir-compatibility</b> is enabled.</p> <p>Workaround: 1. Enter <b>no shut</b> on the affected interfaces before doing an HCCP revertback, or 2. Remove the interface-level HCCP configuration and replace it with a global HCCP configuration.</p>

**Table 59**      **Open Caveats for Cisco IOS Release 12.3(21)BC (continued)**

DDTS ID Number	Description
CSCsg49060	<p>A portion of the modems become unping-able even though they are in the online(pt) state following a Hot Standby Connection-to-Connection Protocol (HCCP) failover.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC2 with a global HCCP configuration.</p> <p>Workaround: Reset each unping-able cable modem (CM), and the CM will return to a working state.</p>
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre data-bbox="574 684 1406 737">SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>

**Table 59**      **Open Caveats for Cisco IOS Release 12.3(21)BC (continued)**

DDTS ID Number	Description
CSCsg61913	<p>When the PXF and IP Multicast are enabled on the Cisco uBR10012 router with the Performance Routing Engine 1 (PRE1) module, the <b>show ip mroute</b> command may not display statistics counters correctly. This limitation is only applied to Cisco uBR10012 router with the PRE1 module.</p> <p>Additional information about IP Multicast is available in the following White Paper on Cisco.com:</p> <ul style="list-style-type: none"> <li>IP MULTICAST IN CABLE NETWORKS  <a href="http://www.cisco.com/en/US/technologies/tk648/tk828/technologies_case_study0900aecd802e2ce2.html">http://www.cisco.com/en/US/technologies/tk648/tk828/technologies_case_study0900aecd802e2ce2.html</a></li> </ul> <p>The following example of the <b>show ip mroute</b> command illustrates typical and proper counter information.</p> <pre>Router# show ip mr count IP Multicast Statistics 8 routes using 4002 bytes of memory 4 groups, 1.00 average sources per group Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)  Group: 225.1.1.1, Source count: 1, Packets forwarded: 119847, Packets received: 23   RP-tree: Forwarding: 29942/1009/28/226, Other: 7/2/0     Source: 60.1.1.2/32, Forwarding: 89905/8988/28/2013, Other: 16/0/0  Group: 224.1.1.1, Source count: 0, Packets forwarded: 0, Packets received: 0  Group: 224.0.1.39, Source count: 1, Packets forwarded: 0, Packets received: 1   Source: 72.2.2.2/32, Forwarding: 0/0/0/0, Other: 1/0/1  Group: 224.0.1.40, Source count: 2, Packets forwarded: 0, Packets received: 2   Source: 72.2.2.2/32, Forwarding: 0/0/0/0, Other: 1/0/1   Source: 72.4.4.4/32, Forwarding: 0/0/0/0, Other: 1/0/1</pre>
CSCsg75417	<p>On an MC520u card, signal-to-noise ratio (SNR) values might drop on an upstream, which could cause modems to drop offline.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC3 with multiple MC520u cards configured for pre-equalization.</p> <p>Workaround: 1. Disable/enable pre-equalization on the upstream. 2. Change the minislot size.</p>

Table 59 Open Caveats for Cisco IOS Release 12.3(21)BC (continued)

DDTS ID Number	Description
CSCsg80760	<p>Cable modems are becoming unpingable within minutes of registration. The modems are still online and DOCSIS pings are successful. Signal-to-noise ratio (SNR) is between around 17dB for 64QAM and 6.4 Mhz channel width.</p> <p>The issue exists on only one upstream at a time. Moving modems from the upstream to another cable line card (CLC) and then back causes the issue to reappear on the same or different upstream. The problem seems to occur only on a 1x8 MAC domain with modems on all 8 upstreams.</p> <p>Workaround: Remove pre-equalization, and reset the CLC.</p>
CSCsg82987	<p>The Simple Network Management Protocol (SNMP) output counters for downstream interfaces and input counters for upstream interfaces are missing for the MC520u0-d card.</p> <p>This issue occurs on a Cisco uBR10000 series router (PRE2-RP) running Cisco IOS Release 12.3(17a)BC2 or 12.3(17a)BC1.</p> <p>There are no known workarounds.</p>
CSCsg87381	<p>When Internetwork Packet Exchange (IPX) packets are sent to a bundle interface, the ifInUnknownPkts counter value remains “0.”</p> <p>There are no known workarounds.</p>
CSCsh05436	<p>Service flows are refused because downstream latency cannot be met by the card.</p> <p>This issue occurs on interfaces having a negative value in the worst case latency for low latency queue, and is caused by using a noncompliant packetcable setup with the packetcable vanilla command. The <b>packetcable authorize vanilla-docsis-mta</b> command allows the receipt of non-compliant service flows. The issue does not occur in a compliant packetcable setup because the “Downstream Latency” value is not permitted.</p> <p>Workaround: Reset the card.</p>
CSCsh11414	<p>A Cisco UBR10000 series router running Cisco IOS Release 12.3(17a)BC2 and configured for Subscriber Account Management Interface Specification (SAMIS) does not save deleted service flows for an offline cable modem if the <b>cable primary-sflow-qos11 keep all</b> command is configured. Consequently, the deleted service flows are absent from the SAMIS and the docsQosServiceFlowLogTable.</p> <p>Workaround: Remove the <b>cable primary-sflow-qos11 keep all</b> command to save the deleted service flow information.</p>
CSCsh24410	<p>After upgrading to Cisco IOS Release 12.3(17b)BC4, some sites report their speed is down.</p> <p>No buffer counters are increased when the <b>show interface command</b> is executed.</p> <p>There are no known workarounds.</p>

**Table 59** *Open Caveats for Cisco IOS Release 12.3(21)BC (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachables" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachables" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh39797	<p>Multicast traffic stops on all modems when acl is configured on a secondary wideband channel. The traffic resumes on all modems after the next igmp query interval.</p> <p>There are no known workarounds.</p>
CSCsh40234	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC6, reports the following message with traceback in the log of the active PRE1 for many different cable modems:</p> <pre>Jan 10 10:29:26 EST: %UBR10000-3-INVALIDSIDPOSITION: Invalid SID (2166) position for interface Cable5/0/0: CM 0011.e358.5d05:Is used by CM 0090.649d.2795 SFID 3679 SID 1834.SID container info: start 8170 end 5766</pre> <p>There are no known workarounds.</p>
CSCsh40309	<p>The burst is not being displayed during a modem upstream (US) trace with Cisco Broadband Troubleshooter (CBT) Version 3.2 when pre-equalization is configured on the US port.</p> <p>This issue occurs only on the 5x20S and U cards when pre-equalization (equalization-coefficient) is configured.</p> <p>This issue doesn't seem to occur on the 28U cards, so it may not be prevalent on the 5x20H either because that card also uses Broadcom for the upstream (US) chip. The TI4522 chip is used on the 5x20S and U cards.</p> <p>Workaround: Do not configure the pre-equalization feature. Note that this feature is off by default.</p>
CSCsh40400	<p>Lower throughput rates occur when the default upstream (US) setting of "token bucket rate limiting with shaping" is enabled.</p> <p>This issue seems to occur because the shaping is causing the rate limiting to kick in too early, resulting in premature delayed grants, and reduced bandwidth.</p> <p>Workaround: Disable shaping and only use token bucket rate limiting if you want to achieve high throughputs in the US.</p>

**Table 59** Open Caveats for Cisco IOS Release 12.3(21)BC (continued)

DDTS ID Number	Description
CSCsh47765	<p>The <b>show hccp brief</b> command may display the same line endlessly under certain combinations of N+1 switchovers.</p> <p>This issue may occur with continuous switchovers in the following sequence:</p> <ol style="list-style-type: none"> <li>1. Switch from W1-&gt;P using “cable power off &lt;W1&gt;” and then power on W1.</li> <li>2. Wait for sync to finish, then switch back to W1 by using power off and turn the power back on.</li> <li>3. Execute the above two steps for W2 LC switch over too.</li> </ol> <p>To resolve this issue, use “cntrlShift 6” and then powering on the W card.</p> <p>There are no known workarounds.</p>
CSCsh50221	<p>The MC5x20 line card crashes on a Cisco uBR10000 series router IOS running Cisco IOS Release 12.3(13a)BC6 because of a bus error exception.</p> <p>There are no known workarounds.</p>
CSCsh51283	<p>Sfid and Dropped counts are missing after Route Processor Redundancy (RPR) switchover.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(21)BC

Table 60 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(21)BC.

**Table 60** Resolved Caveats for Cisco IOS Release 12.3(21)BC

DDTS ID Number	Description
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCej52423	<p>The wrong number of bytes are suppressed and packet drops occur on the dial shelf controller (DSC) when adding payload header suppression (PHS) and line card (LC) switchover.</p> <p>This issue occurs when performing a switchover while using LC redundancy and Multiple PHS for a secondary service flow (SF).</p> <p>Workaround: Do not use PHS with multiple rules for an SF if you are using N+1.</p>

**Table 60 Resolved Caveats for Cisco IOS Release 12.3(21)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCek23320	<p>Simple Network Management Protocol (SNMP)-related traceback occurs when the image is loaded with the attached cable modem termination system (CMTS) configuration:</p> <pre>*Dec 21 16:11:28.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/1, changed state to up Dec 21 16:12:08.141: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61156234 reading 0x0 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 61156234 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 6115623C 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:14:11.138: %AAAA-3-DROPACCTSNDFAIL: Accounting record dropped, send to server failed: system-start</pre> <p>There are no known workarounds.</p>
CSCek24075	<p>Zero nodes are reported in the <b>show srp topology</b> command.</p> <p>There are no known workarounds.</p>
CSCek27678	<p>The <b>show access-list</b> command displays the access control lists (ACLs) for deleted packet filter groups. The corresponding internal ACLs are not removed, even after the packet filter group is deleted.</p> <p>The <b>show cable filter</b> command lists the reserved ACL group 255 index 1 with drop action, even if all the cable filter configurations have been removed from the cable modem termination system (CMTS).</p> <p>There are no known workarounds.</p>
CSCek31526	<p>The Inter-Process Communication (IPC) between cable line cards occasionally fails.</p> <p>Workaround: Reload the image to fix this issue.</p>
CSCek37518	<p>Client information is not displayed in the <b>show cable dsg tunnel ?</b> command when the tunnel group is not associated with a downstream interface.</p> <p>There are no known workarounds.</p>
CSCek38598	<p>No corresponding parallel express forwarding (PXF) queue is created for the new dynamic service flow when testing the dynamic service messaging (DSX) with the <b>test cable DSA</b> command.</p> <p>The real Media Terminal Adapters (MTAs) are able to make call with DSX without any problem.</p> <p>There are no known workarounds.</p>
CSCek39428	<p>DC Directory (DCD) messages do not get captured if the <i>mac-address</i> parameter is specified in the <b>cable monitor</b> command.</p> <p>There are no known workarounds.</p>
CSCek42764	<p>After a line card switchover, the working standby interface configuration is displayed in the <b>show dsg tunnel</b> output.</p> <p>Workaround: Skip the standby interface when scanning cable interfaces to display the DOCSIS Set-Top Gateway (DSG) tunnel information.</p>

**Table 60 Resolved Caveats for Cisco IOS Release 12.3(21)BC (continued)**

DDTS ID Number	Description
CSCek57932	<p>Cisco uBR10012 series devices automatically enable Simple Network Management Protocol (SNMP) read/write access to the device if configured for linecard redundancy. This can be exploited by an attacker to gain complete control of the device. Only Cisco uBR10012 series devices that are configured for linecard redundancy are affected.</p> <p>Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr</a></p>
CSCsa64533	<p>The default modulation profiles for the MC5x20 line card are not optimized for Voice over IP (VoIP).</p> <p>If the intent is to run PacketCable VoIP with G711 at 20 msec packetization without payload header suppression (PHS), the current default modulation profiles can be very inefficient.</p> <p>Workaround: Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Instead of profile 21, configure profile 22.</li> <li>2. Change the FEC CW size to 232.</li> <li>3. Change the FEC T bytes to 9.</li> <li>4. Repeat these steps for profiles 121 and 221.</li> </ol> <p>Note that other line cards, such as the MC28U, already have optimized modulation profiles.</p>
CSCsb21856	<p>Spectrum groups with discrete frequency entries are not supported on cable line cards containing Advanced Spectrum Management functionality.</p> <p>A warning message should be generated if such a spectrum group is applied to an Advanced Spectrum Management capable upstream port.</p> <p>There are no known workarounds.</p>
CSCsb29361	<p>In some circumstances, a cable modem with a downstream minimum reserved rate is allowed to register on a Cisco uBR10000 series cable modem termination system (CMTS). However, committed information rate (CIR) resources for the modem are not available. Error messages similar to the following are displayed in the unit's log:</p> <pre data-bbox="574 1541 1479 1640">%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow 236, CM 0004.9e95.f2a9</pre> <p>The modem is not able to receive any downstream data.</p> <p>The issue occurs only when the total reserved downstream bandwidth approaches the total available downstream bandwidth.</p> <p>There are no known workarounds.</p>

**Table 60 Resolved Caveats for Cisco IOS Release 12.3(21)BC (continued)**

DDTS ID Number	Description
CSCsc12507	<p>When PacketCable event messaging is enabled, the cable modem termination system (CMTS) always uses the global routing table to find the route for the dynamically learned record keeping server (RKS) address. As a result, if the RKS IP address is part of a VPN routing/ forwarding (VRF) route table, CMTS fails to do the correct routing for the Remote Authentication Dial-In User Service (RADIUS) accounting messages.</p> <p>This issue occurs on a Cisco uBR10012 CMTS with a Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) based setup.</p> <p>Workaround: Perform a controlled route distribution between the VRF routing table and the global routing table so that the route for RKS server will be available on the global IPV4 routing table.</p>
CSCsc30294	<p>The following traceback occurs when testing line card failover while making a call from a Cisco uBR10000 series router.</p> <pre>Remote CMTS calls in progress CLI switchover working to protect. SLOT 5/0: Oct 25 17:25:20.871: %SCHED-3-STUCKMTMR: Sleep with expired managed timer 62B2ABD4, time 0xE06B58 (00:00:00 ago). -Process= "Dynamic Services Timer Process", ipl= 4, pid= 40 -Traceback= 601306F0 60130B48 60283108</pre> <p>There are no known workarounds.</p>
CSCsc38875	<p>When a downstream cable interface on a Cisco uBR series router cable modem termination system (CMTS) experiences sustained congestion, and a significant portion of the downstream traffic is multicast traffic, Internet Group Management Protocol Version 2 (IGMPv2) Query messages might not be transmitted successfully in the downstream direction on that cable interface.</p> <p>The issue occurs when large volumes of multicast traffic, using groups that are not specified, use the cable interface <b>cable match address</b> command.</p> <p>Workaround: Ensure that all multicast traffic passing through the CMTS is classified with an appropriate <b>cable match address</b> command. This workaround may be effective only on Cisco uBR10000 series routers.</p>
CSCsc81321	<p>The <b>vendor</b> option is missing from the <b>show cable modem</b> command. When specifying an interface, such as <b>show cable modem c4/0 vendor</b>, the <b>vendor</b> option does not work.</p> <p>Workaround: Use a command without a specific interface to get all interfaces, such as the <b>show cable modem vendor</b> command.</p>
CSCsc91717	<p>There is a discrepancy in packet classification between the Fast Ethernet and Gigabit Ethernet interfaces.</p> <p>There are no known workarounds.</p>
CSCsd03740	<p>The <b>cable upstream 0 scheduling type ?</b> command is not synchronized during N+1 switchover.</p> <p>There are no known workarounds.</p>

Table 60 Resolved Caveats for Cisco IOS Release 12.3(21)BC (continued)

DDTS ID Number	Description
CSCsd31970	<p>On a Cisco uBR10000 series CMTS with redundant PRE modules, new interface mode configuration commands entered on the active PRE may not be properly synchronized to the standby PRE if the <b>do show running-configuration</b> command is entered in interface configuration mode.</p> <p>This may lead to a configuration mismatch between the two PRE modules, and may cause difficulty on PRE switchover.</p> <p>Workaround: Refrain from issuing the <b>do show running-configuration</b> command in interface configuration mode, or completely exit interface configuration mode after issuing the command.</p>
CSCsd36652	<p>When configuring line card redundancy by using the <b>global HA</b> commands, duplicate RF-switch slot numbers were configured. This configuration is not allowed.</p> <p>There are no known workarounds.</p>
CSCsd43741	<p>VID data in the entPhysicalHardwareRev MIB displays the wrong value if the data field in EEPROM is missing.</p> <p>This issue affects the Entity MIB in all Cisco uBR10000 software releases, if the VID data field is not programmed.</p> <p>There are no known workarounds.</p>
CSCsd44373	<p>Certain upstream (US) parameters are not copied from a Working cable line card (CLC) to the Protect CLC during a failover under the following conditions: -upstream docsis mode, -upstream modulation profile, -upstream data-backoff.</p> <p>Because the original settings on the Protect CLC remain, it is possible after a failover to have a Data-over-Cable Service Interface Specification (DOCSIS) mode and modulation profile inconsistent with that of the Working CLC prior to the failover. This inconsistency can create problems. For example, if a Time Division Multiple Access (TDMA)-only Working CLC fails over to a Protect CLC configured with Asynchronous Time Division Multiple Access (ATDMA), the cable modems will switch to ATDMA mode. When the Protect fails back to the TDMA-only Working CLC, the cable modems will continue to use ATDMA and lose IP connectivity.</p> <p>There are no known workarounds.</p>
CSCsd77991	<p>A line card on the Cisco uBR10000 series router unexpectedly crashes.</p> <p>This issue occurs when the <b>clear cable modem</b> command is executed for multicast address.</p> <p>Workaround: Do not use the <b>clear cable modem</b> command for multicast addresses.</p>
CSCsd78370	<p>The privacy bit value of the Multicast entries present on the cable modem termination system (CMTS) host database change after a Route Processor Redundancy (RPR) switchover.</p> <p>This issue occurs when adding multicast entries into the CMTS host database but before the RPR Switchover.</p> <p>There are no known workarounds.</p>

**Table 60 Resolved Caveats for Cisco IOS Release 12.3(21)BC (continued)**

DDTS ID Number	Description
CSCsd95113	<p>A cable modem, when enforced with a quality of service (QoS) profile created using the <code>cdxCmtsCmQosProfile</code> MIB, accepts the profile and <b>show cable modem reg</b> shows the modem with the enforced profile. However, the same cable modem, after reset, does not come online with the enforced profile. Instead, it comes online with the default profile. In contrast, the same modem (when enforced with the QoS profile created using the CLI) comes online after reset with the enforced profile, not the default profile.</p> <p>This behavior is the same irrespective of platforms and whether the QoS profile is created using the CLI or Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCse02543	<p>When some modems are in the reject state and a <b>clear cable modem reject delete</b> command is issued, a <code>CM_INCONSISTENCY</code> message is generated.</p> <p>Workaround: Do not use the <b>clear cable modem reject delete</b> command.</p>
CSCse04266	<p>A Cisco uBR10000 series router reset occurs at <code>sch_rp_first_mac_rw_in_chain</code>.</p> <p>This condition occurs on a Cisco uBR10000 series router with PRE2.</p> <p>There are no known workarounds.</p>
CSCse43344	<p>When a lockout of the Working card is followed by online insertion and removal (OIR), the following two problems occur: 1) OIR switches from the Working card to the Protect card, dropping all the cable modems. 2) After the Working card is back from the OIR, traffic stays on the Protect card with the cable modems down, and the Working card has lockout active. Clearing lockout fails, and because the Working card is standby, reverting to the Working card would also fail.</p> <p>There are no known workarounds.</p>
CSCse45342	<p>Configuring cable default-tos-qos10 tos-overwrite and resetting the modem does not create a new qos-profile. The modem comes online with the existing profile.</p> <p>The problem occurs on modems provisioned in Data-over-Cable Service Interface Specification (DOCSIS) 1.0 mode when the default tos-mask and tos-value are configured.</p> <p>There are no known workarounds.</p>
CSCse54378	<p>On a Cisco uBR10000 series router running Cisco IOS image <code>ubr10k-k9p6u2-mz.2006-06-02.123_17_BC</code>, tracebacks are found at <code>sch_rp_download_debug_info</code> when you attempt to configure an already assigned address.</p> <p>There are no known workarounds.</p>
CSCse56676	<p>The <code>cdrqCmtsCmRQDoneNotification</code> trap, which indicates that the cable remote-query function has finished a polling cycle for modems on the cable modem termination system (CMTS), is sent to Simple Network Management Protocol (SNMP) management stations, even when cable specific traps are not configured to be sent to those stations.</p> <p>This condition occurs on a Cisco uBR series CMTS, and can occur on any trap sent, even when the trap is not associated with the SNMP host.</p> <p>There are no known workarounds.</p>

Table 60 Resolved Caveats for Cisco IOS Release 12.3(21)BC (continued)

DDTS ID Number	Description
CSCse67808	<p>The cdpCacheTable contains entries with index 4294967295 that are only available using the Simple Network Management Protocol (SNMP) <b>get-next</b> command. When the <b>get-one</b> command is used to retrieve the same value, the NO_SUCH_INSTANCE_EXCEPTION is returned.</p> <p>This issue appears to be related to the management ethernet port on the secondary Performance Routing Engine (PRE) in a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCse67868	<p>The Simple Network Management Protocol (SNMP) cpmCPUTotalPhysicalIndex object returns valid entPhysicalIndex values for cable line cards when these values are retrieved using the <b>getnext</b> command, but when the <b>getone</b> command is used, the physical index values for the cable line cards (CLCs) are returned as 0.</p> <p>This issue occurs on Cisco uBR10000 series routers with cable line cards and SNMP configured.</p> <p>There are no known workarounds.</p>
CSCse78143	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>show cr10k-rp cable x/y/z sid</b> command does not allow the service identifier (SID) value to be set to values greater than 8176. As a result, queues associated with downstream multicast quality of service (QoS) SIDs cannot be examined.</p> <p>There are no known workarounds.</p>
CSCse80641	<p>The Transparent LAN Service (TLS) feature does not support stacked dot1q tags.</p> <p>This condition occurs when the TLS feature is configured, and the cable modem termination system (CMTS) receives a 1522 bytes packet (including the frame check sequence(FCS)) in the upstream direction that contains an 802.1q tag.</p> <p>There are no known workarounds.</p>
CSCse84566	<p>This is a feature request for enhancing the Admission Control error messages to help analyze complex system test under heavy PC calls for long period of time.</p>
CSCse85188	<p>On a Cisco cable modem termination system (CMTS), the quality of service (QoS) profile value for the maximum downstream burst is not displayed correctly and may not be set correctly after a reload.</p> <p>This issue occurs when the maximum downstream burst for a QoS profile is configured using the <b>cable qos profile n max-ds-burst value</b> command with a <i>value</i> greater than 2147483647. The value will be displayed as a negative number in the <b>show run</b> command output. If the configuration is written to memory, the maximum downstream burst is also saved as a negative number. As a result, this value is not processed correctly when the configuration is processed after a reload.</p> <p>There are no known workarounds. (Note that the <b>cable qos profile</b> command has been deprecated for Data-over-Cable Service Interface Specification (DOCSIS) 1.1 use because DOCSIS 1.1 replaces the QoS profile with a service flow, which is configured using the <b>cable service class</b> command.</p>
CSCse88914	<p>The total of exclusive bandwidth allocated to various service class names of a particular scheduling type exceeds the exclusive allocation configured for that scheduling type.</p> <p>There are no known workarounds.</p>

**Table 60 Resolved Caveats for Cisco IOS Release 12.3(21)BC (continued)**

DDTS ID Number	Description
CSCsf04338	<p>The Cisco uBR series cable modem termination system (CMTS) with cable or bundle subinterfaces configured does not prevent customer premises equipment (CPE) from receiving a Dynamic Host Configuration Protocol (DHCP) offer with an IP address belonging to the wrong subinterface. Only DHCP offers that contain an offered IP address within the same subinterface as the cable modem belonging to the customer premises equipment (CPE) should be forwarded by the CMTS.</p> <p>The issue occurs when the CMTS is configured to use cable or bundle subinterfaces and the DHCP server is misconfigured.</p> <p>Workaround: Ensure that the DHCP server is configured to assign CPE devices IP addresses from only the appropriate IP subnets.</p>
CSCsf04754	<p>Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.</p> <p>The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.</p> <p>Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.</p> <p>This advisory will be posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080610-snmv3">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080610-snmv3</a></p>
CSCsf22037	<p>The cable sflog maximum entry value needs to be changed to 1-59999</p> <p>There are no known workarounds.</p>
CSCsf30877	<p>The wrong classification is applied to the IP Protocol field.</p> <p>There are no known workarounds.</p>
CSCsg41805	<p>A cable modem is not pingable after a reset modem from the cable modem termination system (CMTS). The cable modem gets stuck in the init(d) state and is not able to come online.</p> <p>This issue occurs in Hot Standby Connection-to-Connection Protocol (HCCP) line card redundancy and virtual interface (VI) bundle interface configurations and can occur on the Protect line card after different line card failovers and Route Processor switchovers</p> <p>Workaround: Failover back to the Working line card.</p>
CSCsg80690	<p>When reverting from a Protect U card to a Working H card, most cable modems on 6.4MHz ATDMA DOC 2.0 channels drop offline. Other upstream channels work correctly.</p> <p>This issue typically occurs in 50% of the reverts performed.</p> <p>There are no known workarounds other than to not use 6.4MHz ADMTA channels.</p>

## Open Caveats for Release 12.3(17b)BC8

Table 61 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC8.

**Table 61** Open Caveats for Cisco IOS Release 12.3(17b)BC8

DDTS ID Number	Description
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCej52423	<p>The wrong number of bytes are suppressed and packet drops occur on the dial shelf controller (DSC) when adding payload header suppression (PHS) and line card (LC) switchover.</p> <p>This issue occurs when performing a switchover while using LC redundancy and Multiple PHS for a secondary service flow (SF).</p> <p>Workaround: Do not use PHS with multiple rules for an SF if you are using N+1.</p>
CSCek41611	<p>Cisco uBR10-MC5X20U cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>
CSCek23320	<p>Simple Network Management Protocol (SNMP)-related traceback occurs when the image is loaded with the attached cable modem termination system (CMTS) configuration:</p> <pre>*Dec 21 16:11:28.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/1, changed state to up Dec 21 16:12:08.141: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61156234 reading 0x0 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 61156234 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 6115623C 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:14:11.138: %AAAA-3-DROPACCTSNDFAIL: Accounting record dropped, send to server failed: system-start</pre> <p>There are no known workarounds.</p>
CSCek24075	<p>Zero nodes are reported in the <b>show srp topology</b> command.</p> <p>There are no known workarounds.</p>
CSCek27678	<p>The <b>show access-list</b> command displays the access control lists (ACLs) for deleted packet filter groups. The corresponding internal ACLs are not removed, even after the packet filter group is deleted.</p> <p>The <b>show cable filter</b> command lists the reserved ACL group 255 index 1 with drop action, even if all the cable filter configurations have been removed from the cable modem termination system (CMTS).</p> <p>There are no known workarounds.</p>

**Table 61** Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCek31526	<p>The Inter-Process Communication (IPC) between cable line cards occasionally fails.</p> <p>Workaround: Reload the image to fix this issue.</p>
CSCek38598	<p>No corresponding parallel express forwarding (PXF) queue is created for the new dynamic service flow when testing the dynamic service messaging (DSX) with the <b>test cable DSA</b> command.</p> <p>The real Media Terminal Adapters (MTAs) are able to make call with DSX without any problem.</p> <p>There are no known workarounds.</p>
CSCek39428	<p>DC Directory (DCD) messages do not get captured if the <i>mac-address</i> parameter is specified in the <b>cable monitor</b> command.</p> <p>There are no known workarounds.</p>
CSCek42764	<p>After a line card switchover, the working standby interface configuration is displayed in the <b>show dsd tunnel</b> output.</p> <p>Workaround: Skip the standby interface when scanning cable interfaces to display the DOCSIS Set-Top Gateway (DSG) tunnel information.</p>
CSCek66377	<p>Not all entries are seen for the Protect line card in the MIB table.</p> <p>There are no known workarounds.</p>
CSCsa64533	<p>The default modulation profiles for the MC5x20 line card are not optimized for Voice over IP (VoIP).</p> <p>If the intent is to run PacketCable VoIP with G711at 20 msec packetization without payload header suppression (PHS), the current default modulation profiles can be very inefficient.</p> <p>Workaround: Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Instead of profile 21, configure profile 22.</li> <li>2. Change the FEC CW size to 232.</li> <li>3. Change the FEC T bytes to 9.</li> <li>4. Repeat these steps for profiles 121 and 221.</li> </ol> <p>Note that other line cards, such as the MC28U, already have optimized modulation profiles.</p>
CSCsb21856	<p>Spectrum groups with discrete frequency entries are not supported on cable line cards containing Advanced Spectrum Management functionality.</p> <p>A warning message should be generated if such a spectrum group is applied to an Advanced Spectrum Management capable upstream port.</p> <p>There are no known workarounds.</p>

Table 61 Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCsb29361	<p>In some circumstances, a cable modem with a downstream minimum reserved rate is allowed to register on a Cisco uBR10000 series cable modem termination system (CMTS). However, committed information rate (CIR) resources for the modem are not available. Error messages similar to the following are displayed in the unit's log:</p> <pre>%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow 236, CM 0004.9e95.f2a9</pre> <p>The modem is not able to receive any downstream data.</p> <p>The issue occurs only when the total reserved downstream bandwidth approaches the total available downstream bandwidth.</p> <p>There are no known workarounds.</p>
CSCsc12507	<p>When PacketCable event messaging is enabled, the cable modem termination system (CMTS) always uses the global routing table to find the route for the dynamically learned record keeping server (RKS) address. As a result, if the RKS IP address is part of a VPN routing/ forwarding (VRF) route table, CMTS fails to do the correct routing for the Remote Authentication Dial-In User Service (RADIUS) accounting messages.</p> <p>This issue occurs on a Cisco uBR10012 CMTS with an Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) based setup.</p> <p>Workaround: Perform a controlled route distribution between the VRF routing table and the global routing table so that the route for RKS server will be available on the global IPV4 routing table.</p>
CSCsc30294	<p>The following traceback occurs when testing line card failover while making a call from a Cisco uBR10000 series router.</p> <pre>Remote CMTS calls in progress CLI switchover working to protect. SLOT 5/0: Oct 25 17:25:20.871: %SCHED-3-STUCKMTMR: Sleep with expired managed timer 62B2ABD4, time 0xE06B58 (00:00:00 ago). -Process= "Dynamic Services Timer Process", ipl= 4, pid= 40 -Traceback= 601306F0 60130B48 60283108</pre> <p>There are no known workarounds.</p>
CSCsc35150	<p>If the <b>global hccp config</b> command is re-entered, the specified line card fails over.</p> <p>This issue occurs when you re-enter the <b>global hccp config</b> command and enter <b>Ctrl-Z</b> to exit. This action invokes an enter and exit at the same time and forces a line card failover.</p> <p>Workaround: To parse out the <b>config</b> command, delete the <b>config</b> command before you invoke <b>Ctrl-Z</b> or type <b>exit/end</b>. You can use <b>Ctrl-C</b> also. Either way, don't re-enter a <b>config</b> command that is already entered.</p>

**Table 61** Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCsc38875	<p>When a downstream cable interface on a Cisco uBR series router cable modem termination system (CMTS) experiences sustained congestion, and a significant portion of the downstream traffic is multicast traffic, Internet Group Management Protocol Version 2 (IGMPv2) Query messages might not be transmitted successfully in the downstream direction on that cable interface.</p> <p>The issue occurs when large volumes of multicast traffic, using groups that are not specified, use the cable interface <b>cable match address</b> command.</p> <p>Workaround: Ensure that all multicast traffic passing through the CMTS is classified with an appropriate <b>cable match address</b> command. This workaround may be effective only on Cisco uBR10000 series routers.</p>
CSCsc81321	<p>The <b>vendor</b> option is missing from the <b>show cable modem</b> command. When specifying an interface, such as <b>show cable modem c4/0 vendor</b>, the <b>vendor</b> option does not work.</p> <p>Workaround: Use a command without a specific interface to get all interfaces, such as the <b>show cable modem vendor</b> command.</p>
CSCsc91717	<p>There is a discrepancy in packet classification between the Fast Ethernet and Gigabit Ethernet interfaces.</p> <p>There are no known workarounds.</p>
CSCsd03740	<p>The <b>cable upstream 0 scheduling type ?</b> command is not synchronized during N+1 switchover.</p> <p>There are no known workarounds.</p>
CSCsd31970	<p>On a Cisco uBR10000 series router cable modem termination system (CMTS) with redundant Performance Routing Engine (PRE) modules, new interface mode configuration commands entered on the active PRE may not be properly synchronized to the standby PRE if the <b>do show running-configuration</b> command is entered in interface configuration mode.</p> <p>This issue can lead to a configuration mismatch between the two PRE modules and can cause difficulty on PRE switchover.</p> <p>Workaround: Refrain from issuing the <b>do show running-configuration</b> command in interface configuration mode, or completely exit interface configuration mode after issuing the command.</p>
CSCsd36652	<p>When configuring line card redundancy by using the <b>global HA</b> commands, duplicate RF-switch slot numbers were configured. This configuration is not allowed.</p> <p>There are no known workarounds.</p>
CSCsd43741	<p>VID data in the entPhysicalHardwareRev MIB displays the wrong value if the data field in EEPROM is missing.</p> <p>This issue affects the Entity MIB in all Cisco uBR10000 software releases, if the VID data field is not programmed.</p> <p>There are no known workarounds.</p>

**Table 61** Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCsd44373	<p>Certain upstream (US) parameters are not copied from a Working cable line card (CLC) to the Protect CLC during a failover under the following conditions: upstream docsis mode, upstream modulation profile, and upstream data-backoff.</p> <p>Because the original settings on the Protect CLC remain, it is possible after a failover to have a Data-over-Cable Service Interface Specification (DOCSIS) mode and modulation profile inconsistent with that of the Working CLC prior to the failover. This inconsistency can create problems. For example, if a Time Division Multiple Access (TDMA)-only Working CLC fails over to a Protect CLC configured with Asynchronous Time Division Multiple Access (ATDMA), the cable modems will switch to ATDMA mode. When the Protect fails back to the TDMA-only Working CLC, the cable modems will continue to use ATDMA and lose IP connectivity for a period of time. This delay can further impact PC voice calls.</p> <p>Workaround: Ensure the Protect CLC is configured with the lowest possible denominator with respect to DOCSIS mode and the modulation profile. The problem is triggered only when protect CLC is configured with a DOCSIS mode exceeding that of the Working CLC.</p>
CSCsd77991	<p>A line card on the Cisco uBR10000 series router unexpectedly crashes.</p> <p>This issue occurs when the <b>clear cable modem</b> command is executed for multicast address.</p> <p>Workaround: Do not use the <b>clear cable modem</b> command for multicast addresses.</p>
CSCsd78370	<p>The privacy bit value of the Multicast entries present on the cable modem termination system (CMTS) host database change after a Route Processor Redundancy (RPR) switchover.</p> <p>This issue occurs when adding multicast entries into the CMTS host database but before the RPR Switchover.</p> <p>There are no known workarounds.</p>
CSCsd95113	<p>A cable modem, when enforced with a quality of service (QoS) profile created using the <code>cdxCmtsCmQoSProfile</code> MIB, accepts the profile and <b>show cable modem reg</b> shows the modem with the enforced profile. However, the same cable modem, after reset, does not come online with the enforced profile. Instead, it comes online with the default profile. In contrast, the same modem (when enforced with the QoS profile created using the CLI) comes online after reset with the enforced profile, not the default profile.</p> <p>This behavior is the same irrespective of platforms and whether the QoS profile is created using the CLI or Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCse00902	<p>Various <b>show</b> commands use improper case and spelling.</p> <p>There are no known workarounds.</p>
CSCse02543	<p>When some modems are in the reject state and a <b>clear cable modem reject delete</b> command is issued, a <code>CM_INCONSISTENCY</code> message is generated.</p> <p>Workaround: Do not use the <b>clear cable modem reject delete</b> command.</p>

**Table 61** Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCse43344	<p>When a lockout of the Working card is followed by online insertion and removal (OIR), the following two problems occur: 1) OIR switches from the Working card to the Protect card, dropping all the cable modems. 2) After the Working card is back from the OIR, traffic stays on the Protect card with the cable modems down, and the Working card has lockout active. Clearing lockout fails, and because the Working card is standby, reverting to the Working card would also fail.</p> <p>There are no known workarounds.</p>
CSCse45342	<p>Configuring cable default-tos-qos10 tos-overwrite and resetting the modem does not create a new qos-profile. The modem comes online with the existing profile.</p> <p>The problem occurs on modems provisioned in Data-over-Cable Service Interface Specification (DOCSIS) 1.0 mode when the default tos-mask and tos-value are configured.</p> <p>There are no known workarounds.</p>
CSCse54378	<p>On a Cisco uBR10000 series router running Cisco IOS image ubr10k-k9p6u2-mz.2006-06-02.123_17_BC, tracebacks are found at sch_rp_download_debug_info when you attempt to configure an already assigned address.</p> <p>There are no known workarounds.</p>
CSCse67808	<p>The cdpCacheTable contains entries with index 4294967295 that are only available using the Simple Network Management Protocol (SNMP) <b>get-next</b> command. When the <b>get-one</b> command is used to retrieve the same value, the NO_SUCH_INSTANCE_EXCEPTION is returned.</p> <p>This issue appears to be related to the management ethernet port on the secondary Performance Routing Engine (PRE) in a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCse67868	<p>The Simple Network Management Protocol (SNMP) cpmCPUTotalPhysicalIndex object returns valid entPhysicalIndex values for cable line cards when these values are retrieved using the <b>getnext</b> command, but when the <b>getone</b> command is used, the physical index values for the cable line cards (CLCs) are returned as 0.</p> <p>This issue occurs on Cisco uBR10000 series routers with cable line cards and SNMP configured.</p> <p>There are no known workarounds.</p>
CSCse78143	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>show cr10k-rp cable x/y/z sid</b> command does not allow the service identifier (SID) value to be set to values greater than 8176. As a result, queues associated with downstream multicast quality of service (QoS) SIDs cannot be examined.</p> <p>There are no known workarounds.</p>
CSCse80641	<p>The Transparent LAN Service (TLS) feature does not support stacked dot1q tags.</p> <p>This condition occurs when the TLS feature is configured, and the cable modem termination system (CMTS) receives a 1522 bytes packet (including the frame check sequence (FCS)) in the upstream direction that contains an 802.1q tag.</p> <p>There are no known workarounds.</p>

Table 61 Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCse84566	<p>This is a feature request for enhancing the Admission Control error messages to help analyze complex system test under heavy PC calls for long period of time.</p> <p>There are no known workarounds.</p>
CSCse85188	<p>On a Cisco cable modem termination system (CMTS), the quality of service (QoS) profile value for the maximum downstream burst is not displayed correctly and may not be set correctly after a reload.</p> <p>This issue occurs when the maximum downstream burst for a QoS profile is configured using the <b>cable qos profile n max-ds-burst value</b> command with a <i>value</i> greater than 2147483647. The value will be displayed as a negative number in the <b>show run</b> command output. If the configuration is written to memory, the maximum downstream burst is also saved as a negative number. As a result, this value is not processed correctly when the configuration is processed after a reload.</p> <p>There are no known workarounds. (Note that the <b>cable qos profile</b> command has been deprecated for Data-over-Cable Service Interface Specification (DOCSIS) 1.1 use because DOCSIS 1.1 replaces the QoS profile with a service flow, which is configured using the <b>cable service class</b> command.</p>
CSCse88914	<p>The total of exclusive bandwidth allocated to various service class names of a particular scheduling type exceeds the exclusive allocation configured for that scheduling type.</p> <p>There are no known workarounds.</p>
CSCsf04338	<p>The Cisco uBR series cable modem termination system (CMTS) with cable or bundle subinterfaces configured does not prevent customer premises equipment (CPE) from receiving a Dynamic Host Configuration Protocol (DHCP) offer with an IP address belonging to the wrong subinterface. Only DHCP offers that contain an offered IP address within the same subinterface as the cable modem belonging to the customer premises equipment (CPE) should be forwarded by the CMTS.</p> <p>The issue occurs when the CMTS is configured to use cable or bundle subinterfaces and the DHCP server is misconfigured.</p> <p>Workaround: Ensure that the DHCP server is configured to assign CPE devices IP addresses from only the appropriate IP subnets.</p>
CSCsf22037	<p>The cable sflog maximum entry value needs to be changed to 1-59999</p> <p>There are no known workarounds.</p>
CSCsf30877	<p>The wrong classification is applied to the IP Protocol field.</p> <p>There are no known workarounds.</p>
CSCsg45692	<p>The Cisco uBR10K 5X20 line card crashes at cr10k_clc_pre_poll.</p> <p>This issue occurs on Cisco IOS Release 12.3(13a)BC6 or Cisco IOS Release 12.3(9a)BC7.</p> <p>There are no known workarounds.</p>

**Table 61** Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre data-bbox="613 426 1446 474">SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>
CSCsg74219	<p>When N+1 line card switchover happens in a Cisco UBR10K chassis running 12.3(21)BC, it is possible that dhcp source verification requests may be sent out again, even though the verification has already been performed before the switchover.</p> <p>This issue occurs when <b>cable source verify dhcp</b> is configured on the cable interface on Cisco UBR10K.</p> <p>There are no known workarounds.</p>
CSCsg75417	<p>On an MC520u card, signal-to-noise ratio (SNR) values might drop on an upstream, which could cause modems to drop offline.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC3 with multiple MC520u cards configured for pre-equalization.</p> <p>Workaround: 1. Disable/enable pre-equalization on the upstream. 2. Change the minislot size.</p>
CSCsh20158	<p>On a Cisco uBR series cable modem termination system (CMTS), if the <b>cable source-verify dhcp</b> function receives a NAK in response to a Dynamic Host Configuration Protocol (DHCP) leasequery, it stops sending any more leasequeries until the system performs a successful DHCP release/renew.</p> <p>This issue could potentially stop a legitimate user from getting connectivity for a short period of time.</p> <p>There are no known workarounds.</p>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol data-bbox="613 1486 1516 1724" style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachable" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachable" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>

**Table 61**      **Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh40400	<p>Lower throughput rates occur when the default upstream (US) setting of "token bucket rate limiting with shaping" is enabled.</p> <p>This issue seems to occur because the shaping is causing the rate limiting to kick in too early, resulting in premature delayed grants, and reduced bandwidth.</p> <p>Workaround: Disable shaping and only use token bucket rate limiting if you want to achieve high throughputs in the US.</p>
CSCsh72746	<p>Intermittent bursts of upstream traffic observed on the outgoing WAN interface.</p> <p>This issue occurs with upstream traffic from RF line cards towards WAN interface.</p> <p>There are no known workarounds.</p>
CSCsh72785	<p>No SNMP trap is generated on behalf of the Redundant PRE state change.</p> <p>This issue may occur on the Redundant PRE configuration and state change of redundant unit.</p> <p>There are no known workarounds.</p>
CSCsi20529	<p>When pre-equalization is enabled, modems SNR can drop unexpectedly.</p> <p>It is unknown when this problem may occur.</p> <p>Workaround: Turn off pre-equalization.</p>
CSCsi30772	<p>After upgrade from 12.2BC to 12.3BC, the Packetcable code may start rejecting DSA-Req explicitly containing the poll jitter TLV.</p> <p>Workaround: Either drop the poll jitter altogether or use 12.2BC.</p>
CSCsi33625	<p>The code automatically changes the acceptable upstream power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This is legal for all US channel width options. BTW, the spelling of dBmV is incorrect as well.</p>

**Table 61**      **Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)**

DDTS ID Number	Description
CSCsi83966	<p>Multiple tracebacks are observed:</p> <pre>313861: Apr 10 07:16:06.784 UTC: %REQGRP-3-SYSCALL: System call for command 72 (slot4/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 6069F510 606B35B0 60C5A09C 60C5B7E0 60C58980 61005A70 610093CC 60FF9910 6101FE0C 60916AC4 60916AA8</pre> <pre>314045: Apr 10 08:16:39.940 UTC: %REQGRP-3-SYSCALL: System call for command 42 (slot4/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 6069F510 606AC4A8 606AEED4 60C898A0 60C89B34 60C5AD40 60C5B188 60C5B834 60C58980 61005A70 610093CC 60FF9910 6101FE0C 60916AC4 60916AA8</pre> <pre>313868: Apr 10 07:18:35.833 UTC: %REQGRP-3-SYSCALL: System call for command 47 (slot4/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 6069F510 606B3D0C 606B4930 6069D1EC 6053BEC4 60886370 60897D40 60916AC4 60916AA8</pre> <p>This issue occurs on an UBR7246VXR with MC28U card. BPI and VPN are not configured and no crashinfo is seen on the PRE or line card.</p> <p>Workaround: Reset the affected line card with hardware module stop/start.</p>
CSCsi87821	<p>CMs may re-range with pre-equalization enabled.</p> <p>This issue occurs on a uBR10k with IOS 123-17b.BC4 using mc520u cards and pre-equalization enabled.</p> <p>Workaround: Disable pre-equalization.</p>
CSCsj18695	<p>An Ubr10k router encounters the following error message:</p> <pre>IDT: %PXF_DMA-3-FBB_LINE_CARD: c10k_chk_ipm() rp_over = 1 ipm_over = 0 slot 18</pre> <p>This issue has been seen to either unexpectedly reload the pxf or cause errors on the router which will lead to the router unexpectedly reloading.</p> <p>This issue has only been observed on an Ubr10k router.</p> <p>There are no known workarounds.</p>
CSCsj20998	<p>The crashinfo file of the UBR10000 may be incomplete. Extra information that is used for debugging unexpected reloads may not be included in the crashinfo file.</p> <p>There are no known workarounds.</p>
CSCsj30057	<p>The CMTS responds slowly to the CLI until the 520u LC is reset through the CLI.</p> <p>The 520u line card may reset due to the following:</p> <pre>%REQGRP-3-SYSCALL: System call for command 43 (slot6/0) : Nonblocking request failed (Cause: timeout)</pre> <p>This issue occurs on an uBR10k running 12.3(17b)BC4 with 520u.</p> <p>Workaround: Reset the LC through the CLI.</p>

**Table 61** Open Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCsj31548	<p>When a U card is replaced with a H card, all Broadcom 3300 based modem have packet loss. This issue is not seen with the U cards.</p> <p>This issue occurs when a U card is replaced with a H card.</p> <p>Workaround: Set the preamble length for station and initial IUCs to 100 bits (50 symbols).</p>
CSCsj36054	<p>The link LED on HH-1GE(uBR10k) remains green despite issuing the <b>shutdown</b> command. The link LED also remains green despite disconnecting the fiber cable.</p> <p>These issues are seen on a 12.3(13a)BC6, 12.3(21a)BC1 or 12.3(21a)BC2 with PRE2(uBR10K) with a Half-Height Gigabit Ethernet Line Card on slot3/0 or 4/0.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(17b)BC8

Table 62 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC8.

**Table 62** Resolved Caveats for Cisco IOS Release 12.3(17b)BC8

DDTS ID Number	Description
CSCeg62070	<p>Tracebacks or unexpected reloads are seen during a HTTP transactions with long URLs.</p> <p>The unexpected reload is seen when the length of any token in the URL of the request is excessively long.</p> <p>Workaround: Disable HTTP server using the <b>no ip http server</b> command.</p>
CSCek57932	<p>Cisco uBR10012 series devices automatically enable Simple Network Management Protocol (SNMP) read/write access to the device if configured for linecard redundancy. This can be exploited by an attacker to gain complete control of the device. Only Cisco uBR10012 series devices that are configured for linecard redundancy are affected.</p> <p>Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr</a></p>
CSCek68815	<p>The <b>show cable modem vendor summary</b> causes memory leak of 4000 bytes per execution on the PRE.</p> <p>Workaround: Avoid the use of the <b>show cable modem vendor summary</b> command.</p>

Table 62 Resolved Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCek77979	<p>When an US is configured with 6.4mhz channel width, many modems go offline in an N+1 SO.</p> <p>The issue might be seen less frequently in a 3.2MHz channel configuration.</p> <p>The issue may not happen in every LC switchover, but it happens sometimes. There has to be a mix of MC520S or MC520U cards with MC520H cards. In this case the H cards was the Protect one in a N+1 solution.</p> <p>Workaround: Have Linecards with the same type for an N+1 solution.</p>
CSCsb78975	<p>The output of <b>show cable modem connectivity</b> display huge value as followings;</p> <pre> Prim  1st time      Times  %online      Online time          Offline time Sid   online         Online           min    avg    max    min    avg max 9     04:45:02      1      100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 11    04:45:02      1      100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 </pre> <p>This issue may occur during PRE-switchover.</p> <p>There are no known workarounds.</p>
CSCsb79076	<p>%SYS-3-TIMERNEG errors and tracebacks are observed while making MGCP RSVP calls on a analog (RGW) setups.</p> <p>This is observed in 12.4(3.9)T1 IOS version.</p> <p>There are no known workarounds.</p>
CSCsd67236	<p>A policy-based routing (PBR) map with a set clause does not act on matching packets.</p> <p>This issue occurs on PRE1s on Cisco uBR10000 series routers only.</p> <p>There are no known workarounds.</p>
CSCse56501	<p>A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.</p> <p>Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.</p> <p>This advisory is posted at  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6</a></p>

Table 62 Resolved Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)

DDTS ID Number	Description
CSCse61661	<p>The dynamic flow is not mapped to the configured virtual routing and forwarding VRF instance if <b>cable dynamic-flow vrf name</b> is configured at the interface level. The mapping works correctly if <b>cable dynamic-flow vrf name</b> is configured globally. The configuration works correctly for a regular physical interface, but does not work on a bundle interface.</p> <p>There are no known workarounds.</p>
CSCsg16291	<p>The following error is seen when performing a switchover from PRE B back to PRE A using the CLI redundancy force-failover main-cpu:</p> <pre>R7278-PRE2#redundancy force-failover ? % Unrecognized command R7278-PRE2#redundancy force-failover ? % Unrecognized command R7278-PRE2#redundancy force-failover % Incomplete command.</pre> <p>There are no known workarounds.</p>
CSCsg26525	<p>Some BadEnqueue tracebacks messages is observed as followings;</p> <pre>SLOT 8/0: %SYS-2-LINKED: Bad enqueue of 623F61A8 in queue 617947D8 -Process= "CMTS MAC Protocol", ipl= 3, pid= 38 -Traceback= 60150138 60214164 602877A0 60220FA8 602129F4 6020E120 6020EA8C 602F03B0</pre> <p>This BadEnqueue message many only be seen one time, or it may be seen continuously.</p> <p>This issue occurs on a cable line card. In worst case scenarios, cable modems trying to register on the affected interface become stuck in the init state. Administratively toggling the interface clears this condition.</p> <p>Workaround: Do not use the cable load-balance function.</p>
CSCsg40567	<p>Malformed SSL packets may cause a router to leak multiple memory blocks.</p> <p>This issue is observed on a Cisco router that has the <b>ip http secure server</b> command enabled.</p> <p>Workaround: Disable the <b>ip http secure server</b> command.</p>
CSCsg64376	<p>A CLI is added to allow engineers to turn on debugging to collect potential inconsistent DOCSIS sync message on the standby PRE:</p> <pre>Router#debug cr10k-rp ha-consistency CR10K RP debug High Availability consistency debugging is on</pre> <p>If an inconsistent DOCSIS sync message is received on the standby PRE, instead of forcing a crash on the standby PRE, a rate-limited warning message like the one below is logged:</p> <pre>00:00:49: %UBR10K_REDUNDANCY-4-RP_HA_STDBY_INCONSISTENT: Standby PRE is in inconsistent state. Error count 1. 7/1 REMOTE BOARD not inserted.</pre> <p>There are no known workarounds.</p>

**Table 62 Resolved Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsg75291	<p>PXF unexpectedly reloads with the following error message:</p> <p>PXF DMA Error - End of Descriptor Before Cmd Byte Length Exhausted</p> <p>See SR 605820247.</p> <p>This issue occurs when ARP packets are punted to RP from the feedback path.</p> <p>There are no known workarounds.</p>
CSCsh75026	<p>On the uBR10000, it is not possible to set the trust point of the manufacturer CA certificates using the CLI.</p> <p>At any time, it is not possible to set a manufacturer CA certificate to Trusted or Untrusted using the configuration.</p> <p>Workaround: As required by DOCSIS, setting the trust point is supported only using SNMP.</p>
CSCsh76002	<p>Service flows failed to get admitted or activated.</p> <p>There are no known workarounds.</p>
CSCsh81152	<p>A Cisco uBR7200 or uBR10000 series CMTS does not allow setting the trust state of the Manufacturer CA certificates via CLI.</p> <p>Setting a Manufacturer CA certificate to untrusted does have any effect. A Manufacturer CA certificate cannot be added to the hotlist, which prevents the operator from being able to prevent a specific manufacturer from registering on the network.</p> <p>Workaround: Use SNMP to set the Manufacturer CA to untrusted.</p>
CSCsi01470	<p>A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.</p> <p>Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.</p> <p>This advisory is posted at <a href="http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-mvpn.html">http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-mvpn.html</a></p>
CSCsi05020	<p>Ubr10k with a bundle interface configured with <b>ip flow ingress</b> and <b>mpls netflow egress</b>. The netflow table only shows the ingress flows, and never the egress.</p> <p>This issue occurs in a ubr10K running 12.3(21)BC, but does not occur in a ubr7206VXR running the same IOS and same configuration.</p> <p>There are no known workarounds.</p>
CSCsi14917	<p>The cable interface falls into Minor alarm due to Physical Port Link Down [0].</p> <p>This issue occurs during PRE switch over.</p> <p>Workaround: Use <b>shut / no shut</b> on the cable interfaces.</p>

**Table 62 Resolved Caveats for Cisco IOS Release 12.3(17b)BC8 (continued)**

DDTS ID Number	Description
CSCsi22189	<p>The ubr10000/PRE2 reported several RP and PXF unexpectedly reloads.</p> <p>The RP reported message:</p> <pre>%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 74BD35C0 data 74BD40E8 chunkmagic 15A3C78B chunk_freemagic 21CD -Process= "Check heaps", ipl= 0, pid= 5 -Traceback= 6066FEB0 60670054 6067F120</pre> <p>While the PXF unexpected reloads with the message:</p> <pre>Feb 27 20:29:20.785: %UBR10000-6-BADIPSOURCE_BUNDLE: Interface Cable7/0/3, IP packet from invalid source. IP=89.216.182.46, MAC=0018.f85a.7095, Expected Interface=Cable7/0/1 SID=455, Actual Interface=Cable7/0/3 SID=755</pre> <pre>=== Start of Toaster Crashinfo Collection (20:29:21 CET Tue Feb 27 2007) === PXF DMA OQC at End of Descriptor With Non-Zero Continuation Bit</pre> <p>There are no known workarounds.</p>
CSCsi26894	<p>After two or more of PRE switchovers by the admin for IOS upgrade, all CMs connected to the systems will encounter download speeds less than 1Mbps.</p> <p>This issue occurs whenever two or more PRE switchovers are executed. This error occurred in 12.3(17b)BC3 and BC5. When tested in 12.3(13a)BC3 and 12.3(21)BC, there was no problem.</p> <p>Workaround: Performing a CM disconnect and reconnect solves this problem.</p>
CSCsi27520	<p>The following interface RPF configuration commands are accepted on the ubr10k even though they are not supported in the ubr10k microcode:</p> <pre>ip unicast source reachable-via any allow-default ip unicast source reachable-via rx &lt;1-199&gt; ip unicast source reachable-via rx &lt;1300-2699&gt;</pre> <p>Workaround: Do not configure the unsupported commands.</p>
CSCsi67793	<p>Cable ARP Filtering in PXF only reports filtering by service identifier (SID) when issued a command <b>show cable arp-filter</b>.</p> <p>It should display a majority of the “M/S” columns with MAC address and “Pro” field should show “PXF”</p> <p>There are no known workarounds.</p>
CSCsj18516	<p>CMTS does not allow more than 8 downstream service flows with PHS enabled for a single modem.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(17b)BC7

Table 63 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC7.

**Table 63** Open Caveats for Cisco IOS Release 12.3(17b)BC7

DDTS ID Number	Description
CSCek21720	<p>Traceback occurs with packet intercept during a line card (LC) switchover in PRE2.</p> <p>This issue occurs when the LC switchover is performed while PacketCable (PC) calls and class features are in progress.</p> <p>There are no known workarounds.</p>
CSCek64423	<p>The cable line card may power up again when a <b>cable power off</b> command is issued.</p> <p>There are no known workarounds.</p>
CSCek68447	<p>While making PC/PCMM calls, the standby PRE leaks about 100 bytes of memory for every call.</p> <p>There are no known workarounds.</p>
CSCek71992	<p>The MC5x20 line card may unexpectedly reload during HCCP switchover.</p> <p>There are no known workarounds.</p>
CSCsb78975	<p>The output of <b>show cable modem connectivity</b> display huge value as followings;</p> <pre> Prim  1st time    Times  %online    Online time                Offline time Sid   online      Online      min    avg    max    min    avg max 9     04:45:02     1         100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 11    04:45:02     1         100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 </pre> <p>This issue may occur during PRE-switchover.</p> <p>There are no known workarounds.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsc99211	<p>After switchover, some modems go offline and some calls are dropped.</p> <p>This issue occurs after a line card switchover.</p> <p>There are no known workarounds.</p>

**Table 63** Open Caveats for Cisco IOS Release 12.3(17b)BC7 (continued)

DDTS ID Number	Description
CSCse69641	<p>When the <b>show cable modem s t</b> command is issued soon after a <b>clear cable modem all delete</b> command, the console and vty get stuck.</p> <p>The issue occurs in large-scale environments with more than 5000 modems.</p> <p>Workaround: Do not use the <b>clear cable modem all delete</b> command; delete specific modems instead.</p>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsg17050	<p>The DOCSIS Set-Top Gateway (DSG) interface configuration is not retained when a 5X20S card is replaced with a 5x20U card, and vice versa.</p> <p>Workaround: Remove the <b>dsg tg</b> configuration from the global configuration, configure it again, and apply the configuration to the interface.</p>
CSCsg44938	<p>On a Cisco uBR10000 series router running an interface-level Hot Standby Connection-to-Connection Protocol (HCCP) configuration, a swap between the MC520H card and MC520u card forces the first JIB's downstreams into the shutdown state. For instance, if you downgrade from the MC520H card to the MC520u card, notice that the MC520u card shut down Cx/y/0 and Cx/y/2 during the building of its configuration.</p> <p>This issue occurs when the Cisco uBR10000 series router is running Cisco IOS Release 12.3(17a)BC2 with an HCCP Interface-Level configuration and <b>cr10k card slot/subslot oir-compatibility</b> is enabled.</p> <p>Workaround: 1. Enter <b>no shut</b> on the affected interfaces before doing an HCCP revertback, or 2. Remove the interface-level HCCP configuration and replace it with a global HCCP configuration.</p>
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre>SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>

**Table 63** Open Caveats for Cisco IOS Release 12.3(17b)BC7 (continued)

DDTS ID Number	Description
CSCsg74219	<p>When N+1 line card switchover happens in a Cisco UBR10K chassis running 12.3(21)BC, it is possible that dhcp source verification requests may be sent out again, even though the verification has already been performed before the switchover.</p> <p>This issue occurs when <b>cable source verify dhcp</b> is configured on the cable interface on Cisco UBR10K.</p> <p>There are no known workarounds.</p>
CSCsh20158	<p>On a Cisco uBR series cable modem termination system (CMTS), if the <b>cable source-verify dhcp</b> function receives a NAK in response to a Dynamic Host Configuration Protocol (DHCP) leasequery, it stops sending any more leasequeries until the system performs a successful DHCP release/renew.</p> <p>This issue could potentially stop a legitimate user from getting connectivity for a short period of time.</p> <p>There are no known workarounds.</p>
CSCsh24533	<p>The router-id for Open Shortest Path First (OSPF) is not getting synchronized in the standby Performance Routing Engine (PRE).</p> <p>Workaround: After PRE switch over, reconfigure a router-id to OSPF.</p>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachable" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachable" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh40309	<p>The burst is not being displayed during a modem upstream (US) trace with Cisco Broadband Troubleshooter (CBT) Version 3.2 when pre-equalization is configured on the US port.</p> <p>This issue occurs only on the 5x20S and U cards when pre-equalization (equalization-coefficient) is configured.</p> <p>This issue doesn't seem to occur on the 28U cards, so it may not be prevalent on the 5x20H either because that card also uses Broadcom for the upstream (US) chip. The TI4522 chip is used on the 5x20S and U cards.</p> <p>Workaround: Do not configure the pre-equalization feature. Note that this feature is off by default.</p>

Table 63 Open Caveats for Cisco IOS Release 12.3(17b)BC7 (continued)

DDTS ID Number	Description
CSCsh41508	<p>The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.</p> <p>There are no known workarounds.</p>
CSCsh66150	<p>The <b>show cable modem connectivity</b> command output is corrupted under some condition.</p> <p>The following example shows a sample output.</p> <pre> ----- show cable modem connectivity ----- Prim 1st time   Times  %online   Online time           Offline time Sid  online      Online      min    avg    max    min    avg max 9    04:45:02    1          100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 11   04:45:02    1          100.00  00:00  49710d6h49710d6h00:00  00:00 00:00 </pre> <p>This issue occurs after PRE switchover.</p> <p>Workaround: Clear cable modem delete.</p>
CSCsh70767	<p>The tunnel interface can not forward upstream traffic and returns an error destination unreachable icmp packet from bundle interface. The source ip addr of icmp packet is 0.0.0.0</p> <p>This issue occurs on a Cisco uBR10k with pre-1 connected with a router for gre tunnel peer.</p> <p>Workaround: Configure the gre tunnel between the cmts uplink port and router.</p>
CSCsh72746	<p>Intermittent bursts of upstream traffic observed on the outgoing WAN interface.</p> <p>This issue occurs with upstream traffic from RF line cards towards WAN interface.</p> <p>There are no known workarounds.</p>
CSCsh72785	<p>No SNMP trap is generated on behalf of the Redundant PRE state change.</p> <p>This issue may occur on the Redundant PRE configuration and state change of redundant unit.</p> <p>There are no known workarounds.</p>
CSCsh75026	<p>On the uBR10000, it is not possible to set the trust point of the manufacturer CA certificates using the CLI.</p> <p>At any time, it is not possible to set a manufacturer CA certificate to Trusted or Untrusted using the configuration.</p> <p>Workaround: As required by DOCSIS, setting the trust point is supported only using SNMP.</p>
CSCsh76002	<p>Service flows failed to get admitted or activated.</p> <p>There are no known workarounds.</p>

**Table 63** Open Caveats for Cisco IOS Release 12.3(17b)BC7 (continued)

DDTS ID Number	Description
CSCsh91566	<p>Wideband cable modems becomes offline after CMTS is issued <b>microcode reload pxf</b>.</p> <p>This issue occurs when a CMTS that has cable modems registered as wideband cable modems is issued <b>microcode reload pxf</b>. When this happens, all the wideband cable modems go offline as seen in <b>show cable modem</b>.</p> <p>Workaround: This condition is cleared after the wideband interfaces are issued:</p> <pre>shutdown no shutdown</pre>
CSCsh95284	<p>UBR 10000 receives the following error messages without any software or hardware changes.</p> <pre>SLOT 7/0: Feb 22 21:22:33.160: %SYS-2-LINKED: Bad enqueue of 62BA698C in queue 61E65540 -Process= "CMTS MAC Protocol", ipl= 3, pid= 37 -Traceback= 60151B04 60218BC4 602950F0 602290B8 60217354 602125D8 60213168 6030A300</pre> <p>Workaround: According to previous cases, use Cu to reseal the module in Slot 7.</p>
CSCsh96105	<p>Under the following conditions, tracebacks are seen and the modem does not come online.</p> <ul style="list-style-type: none"> <li>• HCCP is configured and activated.</li> <li>• A modem changes upstream to an DOCSIS 2.0 only channel.</li> </ul> <p>Workaround: Delete the modem and let it come online again.</p>
CSCsi02451	<p>UBR10K MC5X20H all CM's on US go offline. Turning off pre-equalization gets them working again.</p> <p>This problem commonly occurs when pre-equalization is turned on for many ports. At the same time.</p> <p>Workaround: Turning pre-equalization off/on will get CMs back online. Enable pre-equalization one port at a time.</p>
CSCsi03598	<p>PRE 2 unexpectedly reloads and goes into a loop.</p> <p>This issue occurs when removing the existing flash card from slot1 of PRE2 and inserting another card and performing a dir all.</p> <p>Workaround: Remove the flash card.</p>
CSCsi04244	<p>On Cisco UBR10K with two PREs, when default route is configured, traffic should recover after PRE switchover within 2.5 seconds. If static ARP is configured, the traffic may be dropped for up to 6 seconds in the case of static default route and up to 30 seconds with OSPF generated default route.</p> <p>Static ARP is configured for the IP address of next hop WAN router, specified as default gateway in the <b>ip route 0.0.0.0 0.0.0.0 &lt;a.b.c.d&gt;</b> command.</p> <p>Workaround: Remove static ARP and use dynamic ARP for next hop router IP address on WAN side.</p>

**Table 63** Open Caveats for Cisco IOS Release 12.3(17b)BC7 (continued)

DDTS ID Number	Description
CSCsi10153	<p>On a UBR10k, running 12.3(17a)BC2, traffic which is directed to a GRE tunnel is not correctly fragmented. The first packet is send correctly, but the second half of the packet seems to be dropped.</p> <p>There are no known workarounds.</p>
CSCsi13905	<p>L3 multicast traffic fails to reach CPE from CMTS DS.</p> <p>This issue occurs under normal L3 multicast traffic flow conditions when DS mcast traffic is being sent to CPE.</p> <p>There are no known workarounds.</p>
CSCsi14917	<p>The cable interface falls into Minor alarm due to Physical Port Link Down [0].</p> <p>This issue occurs during PRE switch over.</p> <p>Workaround: Use <b>shut / no shut</b> on the cable interfaces.</p>
CSCsi22254	<p>Cable Intercept packets are not sent to the collection server.</p> <p>Workaround: Re-enter the <b>cable intercept</b> command in the interface.</p>
CSCsi26894	<p>After two or more of PRE switchovers by the admin for IOS upgrade, all CMs connected to the systems will encounter download speeds less than 1Mbps.</p> <p>This issue occurs whenever two or more PRE switchovers are executed. This error occurred in 12.3(17b)BC3 and BC5. When tested in 12.3(13a)BC3 and 12.3(21)BC, there was no problem.</p> <p>Workaround: Performing a CM disconnect and reconnect solves this problem.</p>
CSCsi27161	<p>A ubr10k may experience a PXF reload and the routing protocols will go down for 5-10 seconds; but the Cable modems will stay online.</p> <p>This issue occurs on a ubr10k running 12.3(17b)BC3.</p> <p>There are no known workarounds.</p>
CSCsi33625	<p>The code automatically changes the acceptable upstream power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This is legal for all US channel width options. BTW, the spelling of dBmV is incorrect as well.</p>

## Resolved Caveats for Release 12.3(17b)BC7

Table 64 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC7.

**Table 64**      **Resolved Caveats for Cisco IOS Release 12.3(17b)BC7**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsi07120	<p data-bbox="613 310 1526 373">Long ping times up to 1000 ms and spurious memory access while investigating latency problem occurs.</p> <p data-bbox="613 384 1526 426">There are no known workarounds.</p>
CSCsi50134	<p data-bbox="613 436 1526 499">On a uBr10k running Cisco IOS Release 12.3(17b)BC4, the cable monitor may not generate traffic with a MC520H-d card from some specific interfaces.</p> <p data-bbox="613 510 1526 552">This issue is seen with ma c520h-d in uBr10k, but only in slot 7.</p> <p data-bbox="613 562 1526 588">There are no known workarounds.</p>

## Open Caveats for Release 12.3(17b)BC6

Table 65 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC6.

**Table 65** Open Caveats for Cisco IOS Release 12.3(17b)BC6

DDTS ID Number	Description
CSCek21720	<p>Traceback occurs with packet intercept during a line card (LC) switchover in PRE2.</p> <p>This issue occurs when the LC switchover is performed while PacketCable (PC) calls and class features are in progress.</p> <p>There are no known workarounds.</p>
CSCek64423	<p>The cable line card may power up again when a <b>cable power off</b> command is issued.</p> <p>There are no known workarounds.</p>
CSCek68447	<p>While making PC/PCMM calls, the standby PRE leaks about 100 bytes of memory for every call.</p> <p>There are no known workarounds.</p>
CSCek71992	<p>The MC5x20 line card may unexpectedly reload during HCCP switchover.</p> <p>There are no known workarounds.</p>
CSCsb78975	<p>The output of <b>show cable modem connectivity</b> display huge value as followings;</p> <pre> Prim  1st time    Times  %online    Online time                Offline time Sid  online      Online      min    avg    max    min    avg max 9    04:45:02    1         100.00  00:00  49710d6h49710d6h00:00    00:00 00:00 11   04:45:02    1         100.00  00:00  49710d6h49710d6h00:00    00:00 00:00                     </pre> <p>This issue may occur during PRE-switchover.</p> <p>There are no known workarounds.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>

**Table 65** Open Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)

DDTS ID Number	Description
CSCsc99211	<p>After switchover, some modems go offline and some calls are dropped.</p> <p>This issue occurs after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCse69641	<p>When the <b>show cable modem s t</b> command is issued soon after a <b>clear cable modem all delete</b> command, the console and vty get stuck.</p> <p>The issue occurs in large-scale environments with more than 5000 modems.</p> <p>Workaround: Do not use the <b>clear cable modem all delete</b> command; delete specific modems instead.</p>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsg17050	<p>The DOCSIS Set-Top Gateway (DSG) interface configuration is not retained when a 5X20S card is replaced with a 5x20U card, and vice versa.</p> <p>Workaround: Remove the <b>dsg tg</b> configuration from the global configuration, configure it again, and apply the configuration to the interface.</p>
CSCsg44938	<p>On a Cisco uBR10000 series router running an interface-level Hot Standby Connection-to-Connection Protocol (HCCP) configuration, a swap between the MC520H card and MC520u card forces the first JIB's downstreams into the shutdown state. For instance, if you downgrade from the MC520H card to the MC520u card, notice that the MC520u card shut down Cx/y/0 and Cx/y/2 during the building of its configuration.</p> <p>This issue occurs when the Cisco uBR10000 series router is running Cisco IOS Release 12.3(17a)BC2 with an HCCP Interface-Level configuration and <b>cr10k card slot/subslot oir-compatibility</b> is enabled.</p> <p>Workaround: 1. Enter <b>no shut</b> on the affected interfaces before doing an HCCP revertback, or 2. Remove the interface-level HCCP configuration and replace it with a global HCCP configuration.</p>
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre data-bbox="613 1738 1523 1791">SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>

Table 65 Open Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)

DDTS ID Number	Description
CSCsg74219	<p>When N+1 line card switchover happens in a Cisco UBR10K chassis running 12.3(21)BC, it is possible that dhcp source verification requests may be sent out again, even though the verification has already been performed before the switchover.</p> <p>This issue occurs when <b>cable source verify dhcp</b> is configured on the cable interface on Cisco UBR10K.</p> <p>There are no known workarounds.</p>
CSCsh20158	<p>On a Cisco uBR series cable modem termination system (CMTS), if the <b>cable source-verify dhcp</b> function receives a NAK in response to a Dynamic Host Configuration Protocol (DHCP) leasequery, it stops sending any more leasequeries until the system performs a successful DHCP release/renew.</p> <p>This issue could potentially stop a legitimate user from getting connectivity for a short period of time.</p> <p>There are no known workarounds.</p>
CSCsh24533	<p>The router-id for Open Shortest Path First (OSPF) is not getting synchronized in the standby Performance Routing Engine (PRE).</p> <p>Workaround: After PRE switch over, reconfigure a router-id to OSPF.</p>
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachable" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachable" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh40309	<p>The burst is not being displayed during a modem upstream (US) trace with Cisco Broadband Troubleshooter (CBT) Version 3.2 when pre-equalization is configured on the US port.</p> <p>This issue occurs only on the 5x20S and U cards when pre-equalization (equalization-coefficient) is configured.</p> <p>This issue doesn't seem to occur on the 28U cards, so it may not be prevalent on the 5x20H either because that card also uses Broadcom for the upstream (US) chip. The TI4522 chip is used on the 5x20S and U cards.</p> <p>Workaround: Do not configure the pre-equalization feature. Note that this feature is off by default.</p>

**Table 65**      **Open Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh41508	<p>The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.</p> <p>There are no known workarounds.</p>
CSCsh66150	<p>The <b>show cable modem connectivity</b> command output is corrupted under some condition.</p> <p>The following example shows a sample output.</p> <pre> ----- show cable modem connectivity ----- Prim 1st time   Times %online   Online time           Offline time Sid  online      Online      min   avg   max   min   avg max 9    04:45:02    1    100.00 00:00 49710d6h49710d6h00:00 00:00 00:00 11   04:45:02    1    100.00 00:00 49710d6h49710d6h00:00 00:00 00:00 </pre> <p>This issue occurs after PRE switchover.</p> <p>Workaround: Clear cable modem delete.</p>
CSCsh70767	<p>The tunnel interface can not forward upstream traffic and returns an error destination unreachable icmp packet from bundle interface. The source ip addr of icmp packet is 0.0.0.0</p> <p>This issue occurs on a Cisco uBR10k with pre-1 connected with a router for gre tunnel peer.</p> <p>Workaround: Configure the gre tunnel between the cmts uplink port and router.</p>
CSCsh72746	<p>Intermittent bursts of upstream traffic observed on the outgoing WAN interface.</p> <p>This issue occurs with upstream traffic from RF line cards towards WAN interface.</p> <p>There are no known workarounds.</p>
CSCsh72785	<p>No SNMP trap is generated on behalf of the Redundant PRE state change.</p> <p>This issue may occur on the Redundant PRE configuration and state change of redundant unit.</p> <p>There are no known workarounds.</p>
CSCsh75026	<p>On the uBR10000, it is not possible to set the trust point of the manufacturer CA certificates using the CLI.</p> <p>At any time, it is not possible to set a manufacturer CA certificate to Trusted or Untrusted using the configuration.</p> <p>Workaround: As required by DOCSIS, setting the trust point is supported only using SNMP.</p>
CSCsh76002	<p>Service flows failed to get admitted or activated.</p> <p>There are no known workarounds.</p>

Table 65 Open Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)

DDTS ID Number	Description
CSCsh91566	<p>Wideband cable modems becomes offline after CMTS is issued <b>microcode reload pxf</b>.</p> <p>This issue occurs when a CMTS that has cable modems registered as wideband cable modems is issued <b>microcode reload pxf</b>. When this happens, all the wideband cable modems go offline as seen in <b>show cable modem</b>.</p> <p>Workaround: This condition is cleared after the wideband interfaces are issued:</p> <pre>shutdown no shutdown</pre>
CSCsh95284	<p>UBR 10000 receives the following error messages without any software or hardware changes.</p> <pre>SLOT 7/0: Feb 22 21:22:33.160: %SYS-2-LINKED: Bad enqueue of 62BA698C in queue 61E65540 -Process= "CMTS MAC Protocol", ipl= 3, pid= 37 -Traceback= 60151B04 60218BC4 602950F0 602290B8 60217354 602125D8 60213168 6030A300</pre> <p>Workaround: According to previous cases, use Cu to reseat the module in Slot 7.</p>
CSCsh96105	<p>Under the following conditions, tracebacks are seen and the modem does not come online.</p> <ul style="list-style-type: none"> <li>• HCCP is configured and activated.</li> <li>• A modem changes upstream to an DOCSIS 2.0 only channel.</li> </ul> <p>Workaround: Delete the modem and let it come online again.</p>
CSCsi02451	<p>UBR10K MC5X20H all CMs on US go offline. Turning off pre-equalization gets them working again.</p> <p>This problem commonly occurs when pre-equalization is turned on for many ports. At the same time.</p> <p>Workaround: Turning pre-equalization off/on will get CMs back online. Enable pre-equalization one port at a time.</p>
CSCsi03598	<p>PRE 2 unexpectedly reloads and goes into a loop.</p> <p>This issue occurs when removing the existing flash card from slot1 of PRE2 and inserting another card and performing a dir all.</p> <p>Workaround: Remove the flash card.</p>
CSCsi04244	<p>On Cisco UBR10K with two PREs, when default route is configured, traffic should recover after PRE switchover within 2.5 seconds. If static ARP is configured, the traffic may be dropped for up to 6 seconds in the case of static default route and up to 30 seconds with OSPF generated default route.</p> <p>Static ARP is configured for the IP address of next hop WAN router, specified as default gateway in the <b>ip route 0.0.0.0 0.0.0.0 &lt;a.b.c.d&gt;</b> command.</p> <p>Workaround: Remove static ARP and use dynamic ARP for next hop router IP address on WAN side.</p>

**Table 65**      **Open Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)**

DDTS ID Number	Description
CSCsi10153	<p>On a UBR10k, running 12.3(17a)BC2, traffic which is directed to a GRE tunnel is not correctly fragmented. The first packet is send correctly, but the second half of the packet seems to be dropped.</p> <p>There are no known workarounds.</p>
CSCsi13905	<p>L3 multicast traffic fails to reach CPE from CMTS DS.</p> <p>This issue occurs under normal L3 multicast traffic flow conditions when DS mcast traffic is being sent to CPE.</p> <p>There are no known workarounds.</p>
CSCsi14917	<p>The cable interface falls into Minor alarm due to Physical Port Link Down [0].</p> <p>This issue occurs during PRE switch over.</p> <p>Workaround: Use <b>shut / no shut</b> on the cable interfaces.</p>
CSCsi22254	<p>Cable Intercept packets are not sent to the collection server.</p> <p>Workaround: Re-enter the <b>cable intercept</b> command in the interface.</p>
CSCsi26894	<p>After two or more of PRE switchovers by the admin for IOS upgrade, all CMs connected to the systems will encounter download speeds less than 1Mbps.</p> <p>This issue occurs whenever two or more PRE switchovers are executed. This error occurred in 12.3(17b)BC3 and BC5. When tested in 12.3(13a)BC3 and 12.3(21)BC, there was no problem.</p> <p>Workaround: Performing a CM disconnect and reconnect solves this problem.</p>
CSCsi27161	<p>A ubr10k may experience a PXF reload and the routing protocols will go down for 5-10 seconds; but the Cable modems will stay online.</p> <p>This issue occurs on a ubr10k running 12.3(17b)BC3.</p> <p>There are no known workarounds.</p>
CSCsi33625	<p>The code automatically changes the acceptable upstream power range when the channel width is already set. If the channel width is changed, there is no check to see if that power level is a legal entry for the new channel width. The running configuration will indicate the illegal entry, but the actual readings at the CMTS US port may not correlate.</p> <p>This issue occurs when US channel width configuration changes are made.</p> <p>Workaround: Always use the default US power-level setting of 0 dBmV. This is legal for all US channel width options. BTW, the spelling of dBmV is incorrect as well.</p>

## Resolved Caveats for Release 12.3(17b)BC6

Table 66 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC6.

**Table 66** Resolved Caveats for Cisco IOS Release 12.3(17b)BC6

DDTS ID Number	Description
CSCek65980	<p>The <b>cops listener access-list</b> command disappears from the running configuration after a cable modem termination system (CMTS) reload, however, it stays in startup configuration.</p> <p>Workaround: Issue the <b>cops listener access-list <i>acl-num</i></b> command after the router boots up.</p>
CSCsd20683	<p>A command switchover with a virtual interface (VI) configuration is not switching the whole line card.</p> <p>By default, when VI is enabled on an interface, the Hot Standby Connection-to-Connection Protocol (HCCP) line card should switchover the whole line card instead of switching an individual domain.</p> <p>There are no known workarounds.</p>
CSCsd30267	<p>The Authentication, Authorization, and Accounting (AAA) per user process is holding memory, and the router is running out of memory.</p> <p>This issue occurs when PPP over Ethernet (PPPoE) dialing and dynamic access control lists (ACLs) are present.</p> <p>There is no known workaround.</p>

**Table 66 Resolved Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)**

DDTS ID Number	Description
CSCsd85587	<p>A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).</p> <p>Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.</p> <p>The vulnerable cryptographic library is used in the following Cisco products:</p> <p>Cisco IOS, documented as Cisco bug ID CSCsd85587</p> <p>Cisco IOS XR, documented as Cisco bug ID CSCsg41084</p> <p>Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999</p> <p>Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348</p> <p>Cisco Firewall Service Module (FWSM)</p> <p>This vulnerability is also being tracked by CERT/CC as VU#754281.</p> <p>Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto</a></p> <p>Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at <a href="http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml</a> and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL</a></p>
CSCsd95616	<p>Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-multicast">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-multicast</a></p>

Table 66 Resolved Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)

DDTS ID Number	Description
CSCse04560	<p>A TFTP client trying to transfer a file from a Cisco IOS device configured as a tftp server and which is denied by an ACL receives a different result depending if the file is being offered for download or not. This may allow a third party to enumerate which files are available for download.</p> <p>The <b>tftp-server</b> command is configured on the device and an ACL restricting access to the file in question has been applied as in this example:</p> <pre>tftp-server flash: filename1 access-list-number access-list access-list-number permit 192.168.1.0 0.0.0.255 access-list access-list-number deny any</pre> <p>Workaround: The following workarounds can be applied:</p> <ol style="list-style-type: none"> <li>1. Interface ACL <p>Configure and attach an access list to every router interface active and configured for IP packet processing. Once the tftp server in Cisco IOS is enabled and listening by default on all interfaces enabled for IP processing, the access list would need to deny traffic to each and every IP address assigned to any active router interface.</p> </li> <li>2. Control Plane Policing <p>Configure and apply a CoPP policy.</p> <p>Note: CoPP is only available on certain platforms and Cisco IOS releases. Additional information on the configuration and use of the CoPP feature can be found at the following URL:</p> <p><a href="http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html">http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html</a></p> </li> <li>3. Infrastructure ACLs (iACL) <p>Although often difficult to block traffic transitting your network, identifying traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network is possible. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for iACLs:</p> <p><a href="http://www.cisco.com/warp/public/707/iacl.html">http://www.cisco.com/warp/public/707/iacl.html</a></p> </li> <li>4. Configuring Receive Access Lists (rACLs) <p>For distributed platforms, rACLs may be an option starting in Cisco IOS Release 12.0(21)S2 for the Cisco 12000 series GSR and Cisco IOS Release 12.0(24)S for the Cisco 7500 series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path ACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help identify and allow legitimate traffic to your device and deny all unwanted packets:</p> <p><a href="http://www.cisco.com/warp/public/707/racl.html">http://www.cisco.com/warp/public/707/racl.html</a></p> </li> </ol>

**Table 66** *Resolved Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCse04894	<p>Setting the lockout flag on the Working line card and then performing a <b>hw-module slot <i>x/y</i> reset</b> of the line card causes a switchover from the Working to the Protect line card, disables the upconverter on the Active Protect line card, and causes all modems to go offline.</p> <p>There are no known workarounds.</p>
CSCse05736	<p>A router running RCP can be reloaded by a specific packet.</p> <p>This issue is seen under the following conditions:</p> <ul style="list-style-type: none"> <li>• The router must have RCP enabled.</li> <li>• The packet must come from the source address of the designated system configured to send RCP packets to the router.</li> <li>• The packet must have a specific data content.</li> </ul> <p>Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.</p>
CSCse56676	<p>The <code>cdrqCmtsCmRQDoneNotification</code> trap, which indicates that the cable remote-query function has finished a polling cycle for modems on the cable modem termination system (CMTS), is sent to Simple Network Management Protocol (SNMP) management stations, even when cable specific traps are not configured to be sent to those stations.</p> <p>This condition occurs on a Cisco uBR series CMTS, and can occur on any trap sent, even when the trap is not associated with the SNMP host.</p> <p>There are no known workarounds.</p>
CSCsg41805	<p>A cable modem is not pingable after a reset modem from the cable modem termination system (CMTS). The cable modem gets stuck in the <code>init(d)</code> state and is not able to come online.</p> <p>This issue occurs in Hot Standby Connection-to-Connection Protocol (HCCP) line card redundancy and virtual interface (VI) bundle interface configurations and can occur on the Protect line card after different line card failovers and Route Processor switchovers</p> <p>Workaround: Failover back to the Working line card.</p>
CSCsg80690	<p>When reverting from a Protect U card to a Working H card, most cable modems on 6.4MHz ATDMA DOC 2.0 channels drop offline. Other upstream channels work correctly.</p> <p>This issue typically occurs in 50% of the reverts performed.</p> <p>There are no known workarounds other than to not use 6.4MHz ADMTA channels.</p>

Table 66 Resolved Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)

DDTS ID Number	Description
CSCsh05436	<p>Service flows are refused because downstream latency cannot be met by the card.</p> <p>This issue occurs on interfaces having a negative value in the worst case latency for low latency queue, and is caused by using a noncompliant packetcable setup with the packetcable vanilla command. The <b>packetcable authorize vanilla-docsis-mta</b> command allows the receipt of non-compliant service flows. The issue does not occur in a compliant packetcable setup because the "Downstream Latency" value is not permitted.</p> <p>Workaround: Reset the card.</p>
CSCsh11414	<p>A Cisco UBR10000 series router running Cisco IOS Release 12.3(17a)BC2 and configured for Subscriber Account Management Interface Specification (SAMIS) does not save deleted service flows for an offline cable modem if the <b>cable primary-sflow-qos11 keep all</b> command is configured. Consequently, the deleted service flows are absent from the SAMIS and the docsQosServiceFlowLogTable.</p> <p>Workaround: Remove the <b>cable primary-sflow-qos11 keep all</b> command to save the deleted service flow information.</p>
CSCsh29217	<p>Cisco 10000, uBR10012 and uBR7200 series devices use a User Datagram Protocol (UDP) based Inter-Process Communication (IPC) channel that is externally reachable. An attacker could exploit this vulnerability to cause a denial of service (DoS) condition on affected devices. No other platforms are affected.</p> <p>Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc</a></p>
CSCsh73925	<p>A Cisco uBR7200 or uBR10000 series CMTS may lose ip connectivity to CM/CPE devices after removing a secondary IP address on a cable or bundle interface.</p> <p>Removing a secondary ip address causes all ARP entries (associated with primary ip address and remaining secondary ip addresses) on that bundle interface to be deleted. Until the ARP table is rebuilt there could be loss of ip connectivity.</p> <p>Workaround: Ensure that secondary IP addresses are removed during a maintenance window.</p> <p>Another potential workaround would be to segment the CMTS into smaller cable interface bundle groups or to use separate subinterfaces so that a lower number of modems and CPE ARP entries are linked to each subinterface.</p>

**Table 66** *Resolved Caveats for Cisco IOS Release 12.3(17b)BC6 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsh84786	<p>After a PRE switchover on theubr10k, the data path to the cable line cards may fail due to a race condition in determining the primary PRE. L3 data traffic through the cable line card is dropped.</p> <p>This is a race condition which may happen after a PRE switchover from PRE.</p> <p>Workaround: Reset the affected cable line card.</p>
CSCsi13905	<p>L3 multicast traffic fails to reach CPE from CMTS DS.</p> <p>This issue occurs under normal L3 multicast traffic flow conditions when DS mcast traffic is being sent to CPE.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(17b)BC5

Table 67 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC5.

**Table 67** Open Caveats for Cisco IOS Release 12.3(17b)BC5

DDTS ID Number	Description
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCej52423	<p>The wrong number of bytes are suppressed and packet drops occur on the dial shelf controller (DSC) when adding payload header suppression (PHS) and line card (LC) switchover.</p> <p>This issue occurs when performing a switchover while using LC redundancy and Multiple PHS for a secondary service flow (SF).</p> <p>Workaround: Do not use PHS with multiple rules for an SF if you are using N+1.</p>
CSCek21720	<p>Traceback occurs with packet intercept during a line card (LC) switchover in PRE2.</p> <p>This issue occurs when the LC switchover is performed while PacketCable (PC) calls and class features are in progress.</p> <p>There are no known workarounds</p>
CSCek23320	<p>Simple Network Management Protocol (SNMP)-related traceback occurs when the image is loaded with the attached cable modem termination system (CMTS) configuration:</p> <pre>*Dec 21 16:11:28.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/1, changed state to up Dec 21 16:12:08.141: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61156234 reading 0x0 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 61156234 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 6115623C 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 2116:14:11.138: %AAAA-3-DROPACCTSNDFAIL: Accounting record dropped, send to server failed: system-start</pre> <p>There are no known workarounds.</p>
CSCek24075	<p>Zero nodes are reported in the <b>show srp topology</b> command.</p> <p>There are no known workarounds.</p>
CSCek24282	<p>A PacketCable Multimedia (PCMM) gate check fails for dynamic load balancing and so the cable modems with active PCMM voice calls load balance even, if they are not supposed to load balance.</p> <p>There are no known workarounds.</p>

**Table 67** Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCek27678	<p>The <b>show access-list</b> command displays the access control lists (ACLs) for deleted packet filter groups. The corresponding internal ACLs are not removed, even after the packet filter group is deleted.</p> <p>The <b>show cable filter</b> command lists the reserved ACL group 255 index 1 with drop action, even if all the cable filter configurations have been removed from the cable modem termination system (CMTS).</p> <p>There are no known workarounds.</p>
CSCek30621	<p>Wideband modem downstream throughput rate is not yet supported.</p> <p>There are no known workarounds.</p>
CSCek31526	<p>The Inter-Process Communication (IPC) between cable line cards occasionally fails.</p> <p>Workaround: Reload the image to fix this issue.</p>
CSCek35970	<p>The IP ToS/DSCP byte is not overwritten for PacketCable CALEA replicated packets with the value received by GATE-SET COPS messages.</p> <p>There are no known workarounds.</p>
CSCek39428	<p>DC Directory (DCD) messages do not get captured if the <i>mac-address</i> parameter is specified in the <b>cable monitor</b> command.</p> <p>There are no known workarounds.</p>
CSCek41611	<p>Cisco uBR10-MC5X20U cards may experience a silent reload.</p> <p>This issue is observed on a PRE-2 running Cisco IOS Release 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>
CSCek42764	<p>After a line card switchover, the working standby interface configuration is displayed in the <b>show dsgr tunnel</b> output.</p> <p>Workaround: Skip the standby interface when scanning cable interfaces to display the DOCSIS Set-Top Gateway (DSG) tunnel information.</p>
CSCek46057	<p>A bundled multicast mapping table entry is mistakenly marked as NULL when an mroute table is removed from IOS.</p> <p>There are no known workarounds.</p>
CSCek51694	<p>The Dynamic Channel Change (DCC) functionality does not work when moving modem between upstreams.</p> <p>There are no known workarounds.</p>

**Table 67 Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)**

DDTS ID Number	Description
CSCek53938	<p>When executing the cmgen 500 1000 CLI at the cable modem termination system (CMTS), the following errors appeared at the CMTS console:</p> <pre>SLOT 5/0: Aug 24 12:02:48.774: %ALIGN-3-CORRECT: Alignment correction made at 0x6085996C reading 0xC3259DB SLOT 5/0: Aug 24 12:02:48.774: %ALIGN-3-TRACE: -Traceback= 6085996C 6025BC08 60355224 603555F4 6035577C 603565CC 60356644 60357A20 Decode: ----- Enter hex value: 6085996C 6025BC08 60355224 603555F4 6035577C 603565CC 60356644 60357A20 0x6085996C:cmgen_pkt_for_fake_cm(0x60859948)+0x24 0x6025BC08:cmts_monitor_pak(0x6025bad0)+0x138 0x60355224:cmts_jib_handle_snfr_pkt(0x60355188)+0x9c 0x603555F4:cmts_jib_common_rx_intr(0x60355338)+0x2bc 0x6035577C:cmts_jib_snfr_ring_intr(0x6035575c)+0x20 0x603565CC:jib_analyse_intr(0x60356530)+0x9c 0x60356644:cmts_net_interrupt_jib(0x60356624)+0x20 0x60357A20:cmts_jib1(0x60357a20)+0x0</pre> <p>There are no known workarounds.</p>
CSCek61705	<p>The <b>show cable modem counter</b> command does not report downstream byte/packet count for wideband cable modems (WCMs) registered as w-online.</p> <p>Workaround: The <b>show cable modem counters</b> command sums the packets/bytes for each of the modem service flows. Counters for the WCM's individual service flows may be obtained as follows. Use the <b>show cable modem interface Cx/y/z service-flow</b> command to list all the service flows in use for the interface in which the WCM is registered. Use the SFID values reported in this command to identify the downstream service flow(s) for the modem of interest. Then, use the <b>show cable modem interface Cx/y/z service-flow n</b> counters command to view the counters for the specific service flow, where <i>n</i> is one of downstream SFIDs for the WCM.</p>
CSCek65425	<p>Seven warnings appear in the getnext docsQosServiceFlowPkts file.</p> <p>There are no known workarounds.</p>
CSCek65980	<p>The <b>cops listener access-list</b> command disappears from the running configuration after a cable modem termination system (CMTS) reload, however, it stays in startup configuration.</p> <p>Workaround: Issue the <b>cops listener access-list acl-num</b> command after the router boots up.</p>
CSCek66377	<p>Not all entries are seen for the Protect line card in the MIB table.</p> <p>There are no known workarounds.</p>
CSCek66923	<p>The following changes have been made to the debug code:</p> <ul style="list-style-type: none"> <li>• New debug code has been added to <code>cmts_delete_entry()</code> to catch when any application uses this function and leaves a dangling pointer in the <code>SID host_chains</code>.</li> <li>• The deliberate crash from <code>is_cmts_entry_poisoned()</code> has been removed due to the new debug code added in step 1 above.</li> </ul> <p>There are no known workarounds.</p>
CSCin98031	<p>N+1 synchronization does not occur when switching over from the Working card to the Protect card.</p> <p>There are no known workarounds.</p>

**Table 67**      **Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)**

DDTS ID Number	Description
CSCsa64533	<p>The default modulation profiles for the MC5x20 line card are not optimized for Voice over IP (VoIP).</p> <p>If the intent is to run PacketCable VoIP with G711at 20 msec packetization without payload header suppression (PHS), the current default modulation profiles can be very inefficient.</p> <p>Workaround: Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Instead of profile 21, configure profile 22.</li> <li>2. Change the FEC CW size to 232.</li> <li>3. Change the FEC T bytes to 9.</li> <li>4. Repeat these steps for profiles 121 and 221.</li> </ol> <p>Note that other line cards, such as the MC28U, already have optimized modulation profiles.</p>
CSCsb21856	<p>Spectrum groups with discrete frequency entries are not supported on cable line cards containing Advanced Spectrum Management functionality.</p> <p>A warning message should be generated if such a spectrum group is applied to an Advanced Spectrum Management capable upstream port.</p> <p>There are no known workarounds.</p>
CSCsb29361	<p>In some circumstances, a cable modem with a downstream minimum reserved rate is allowed to register on a Cisco uBR10000 series cable modem termination system (CMTS). However, committed information rate (CIR) resources for the modem are not available. Error messages similar to the following are displayed in the unit's log:</p> <pre data-bbox="613 1171 1523 1276">%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow 236, CM 0004.9e95.f2a9</pre> <p>The modem is not able to receive any downstream data.</p> <p>The issue occurs only when the total reserved downstream bandwidth approaches the total available downstream bandwidth.</p> <p>There are no known workarounds.</p>

**Table 67**      **Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)**

DDTS ID Number	Description
CSCsb86099	<p>While performing a switchover, the following error message occurs. After multiple switchovers, the router unexpectedly crashes:</p> <pre>Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC2 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC3 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC4 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US2 Physical Port Link Down</pre> <p>This issue occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>• Performing a Route Processor Redundancy (RPR) switchover using the CLI.</li> <li>• Performing multiple switchovers</li> </ul> <p>There are no known workarounds</p>
CSCsc12507	<p>When PacketCable event messaging is enabled, the cable modem termination system (CMTS) always uses the global routing table to find the route for the dynamically learned record keeping server (RKS) address. As a result, if the RKS IP address is part of a VPN routing/ forwarding (VRF) route table, CMTS fails to do the correct routing for the Remote Authentication Dial-In User Service (RADIUS) accounting messages.</p> <p>This issue occurs on a Cisco uBR10012 CMTS with an Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) based setup.</p> <p>Workaround: Perform a controlled route distribution between the VRF routing table and the global routing table so that the route for RKS server will be available on the global IPV4 routing table.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC2 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>

**Table 67 Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsc30294	<p>The following traceback occurs when testing line card failover while making a call from a Cisco uBR10000 series router.</p> <pre>Remote CMTS calls in progress CLI switchover working to protect. SLOT 5/0: Oct 25 17:25:20.871: %SCHED-3-STUCKMTMR: Sleep with expired managed timer 62B2ABD4, time 0xE06B58 (00:00:00 ago). -Process= "Dynamic Services Timer Process", ipl= 4, pid= 40 -Traceback= 601306F0 60130B48 60283108</pre> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsc35150	<p>If the <b>global hccp config</b> command is re-entered, the specified line card fails over.</p> <p>This issue occurs when you re-enter the <b>global hccp config</b> command and enter <b>Ctrl-Z</b> to exit. This action invokes an enter and exit at the same time and forces a line card failover.</p> <p>Workaround: To parse out the <b>config</b> command, delete the <b>config</b> command before you invoke <b>Ctrl-Z</b> or type <b>exit/end</b>. You can use <b>Ctrl-C</b> also. Either way, don't re-enter a <b>config</b> command that is already entered.</p>
CSCsc38875	<p>When a downstream cable interface on a Cisco uBR series router cable modem termination system (CMTS) experiences sustained congestion, and a significant portion of the downstream traffic is multicast traffic, Internet Group Management Protocol Version 2 (IGMPv2) Query messages might not be transmitted successfully in the downstream direction on that cable interface.</p> <p>The issue occurs when large volumes of multicast traffic, using groups that are not specified, use the cable interface <b>cable match address</b> command.</p> <p>Workaround: Ensure that all multicast traffic passing through the CMTS is classified with an appropriate <b>cable match address</b> command. This workaround may be effective only on Cisco uBR10000 series routers.</p>
CSCsc81321	<p>The <b>vendor</b> option is missing from the <b>show cable modem</b> command. When specifying an interface, such as <b>show cable modem c4/0 vendor</b>, the <b>vendor</b> option does not work.</p> <p>Workaround: Use a command without a specific interface to get all interfaces, such as the <b>show cable modem vendor</b> command.</p>
CSCsc91717	<p>There is a discrepancy in packet classification between the Fast Ethernet and Gigabit Ethernet interfaces.</p> <p>There are no known workarounds.</p>
CSCsd03740	<p>The <b>cable upstream 0 scheduling type ?</b> command is not synchronized during N+1 switchover.</p> <p>There are no known workarounds.</p>

Table 67 Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsd20606	<p>A parallel express forwarding (PXF) restart disables multicast traffic that matches the Multicast Quality of Service (MQoS) configuration.</p> <p>This issue occurs when an MQoS configuration is applied to cable interfaces, and PXF is restarted</p> <p>There are no known workarounds.</p>
CSCsd20683	<p>A command switchover with a virtual interface (VI) configuration is not switching the whole line card.</p> <p>By default, when VI is enabled on an interface, the Hot Standby Connection-to-Connection Protocol (HCCP) line card should switchover the whole line card instead of switching an individual domain.</p> <p>There are no known workarounds.</p>
CSCsd29450	<p>A Protect line card crashes after a sequence of route processor (RP) and LC switchovers.</p> <p>This issue occurs when performing a sequence of LC and Performance Routing Engine (PRE) switchovers.</p> <p>There are no known workarounds</p>
CSCsd30267	<p>The Authentication, Authorization, and Accounting (AAA) per user process is holding memory, and the router is running out of memory.</p> <p>This issue occurs when PPP over Ethernet (PPPoE) dialing and dynamic access control lists (ACLs) are present.</p> <p>There is no known workaround.</p>
CSCsd31970	<p>On a Cisco uBR10000 series router cable modem termination system (CMTS) with redundant Performance Routing Engine (PRE) modules, new interface mode configuration commands entered on the active PRE may not be properly synchronized to the standby PRE if the <b>do show running-configuration</b> command is entered in interface configuration mode.</p> <p>This issue can lead to a configuration mismatch between the two PRE modules and can cause difficulty on PRE switchover.</p> <p>Workaround: Refrain from issuing the <b>do show running-configuration</b> command in interface configuration mode, or completely exit interface configuration mode after issuing the command.</p>
CSCsd36652	<p>When configuring line card redundancy by using the <b>global HA</b> commands, duplicate RF-switch slot numbers were configured. This configuration is not allowed.</p> <p>There are no known workarounds.</p>
CSCsd43741	<p>VID data in the entPhysicalHardwareRev MIB displays the wrong value if the data field in EEPROM is missing.</p> <p>This issue affects the Entity MIB in all Cisco uBR10000 software releases, if the VID data field is not programmed.</p> <p>There are no known workarounds.</p>

**Table 67**      **Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)**

DDTS ID Number	Description
CSCsd44373	<p>Certain upstream (US) parameters are not copied from a Working cable line card (CLC) to the Protect CLC during a failover under the following conditions: upstream docsis mode, upstream modulation profile, and upstream data-backoff.</p> <p>Because the original settings on the Protect CLC remain, it is possible after a failover to have a Data-over-Cable Service Interface Specification (DOCSIS) mode and modulation profile inconsistent with that of the Working CLC prior to the failover. This inconsistency can create problems. For example, if a Time Division Multiple Access (TDMA)-only Working CLC fails over to a Protect CLC configured with Asynchronous Time Division Multiple Access (ATDMA), the cable modems will switch to ATDMA mode. When the Protect fails back to the TDMA-only Working CLC, the cable modems will continue to use ATDMA and lose IP connectivity for a period of time. This delay can further impact PC voice calls.</p> <p>Workaround: Ensure the Protect CLC is configured with the lowest possible denominator with respect to DOCSIS mode and the modulation profile. The problem is triggered only when protect CLC is configured with a DOCSIS mode exceeding that of the Working CLC.</p>
CSCsd47667	<p>The cable meter feature is causing redundancy to fail between PRE2s due to Inter-Process Communication (IPC) timeouts.</p> <p>This issue occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC2 or 12.3(17a)BC.</p> <p>Workaround: Reload the standby PRE2.</p>
CSCsd67236	<p>A policy-based routing (PBR) map with a set clause does not act on matching packets.</p> <p>This issue occurs on PRE1s on Cisco uBR10000 series routers only.</p> <p>There are no known workarounds.</p>
CSCsd77991	<p>A line card on the Cisco uBR10000 series router unexpectedly crashes.</p> <p>This issue occurs when the <b>clear cable modem</b> command is executed for multicast address.</p> <p>Workaround: Do not use the <b>clear cable modem</b> command for multicast addresses.</p>
CSCsd78370	<p>The privacy bit value of the Multicast entries present on the cable modem termination system (CMTS) host database change after a Route Processor Redundancy (RPR) switchover.</p> <p>This issue occurs when adding multicast entries into the CMTS host database but before the RPR Switchover.</p> <p>There are no known workarounds.</p>

Table 67 Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsd95113	<p>A cable modem, when enforced with a quality of service (QoS) profile created using the <code>cdxCmtsCmQosProfile</code> MIB, accepts the profile and <b>show cable modem reg</b> shows the modem with the enforced profile. However, the same cable modem, after reset, does not come online with the enforced profile. Instead, it comes online with the default profile. In contrast, the same modem (when enforced with the QoS profile created using the CLI) comes online after reset with the enforced profile, not the default profile.</p> <p>This behavior is the same irrespective of platforms and whether the QoS profile is created using the CLI or Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCsd98200	<p>Spurious memory access occurs while doing a line card switchover.</p> <p>There are no known workarounds.</p>
CSCse00902	<p>Various <b>show</b> commands use improper case and spelling.</p> <p>There are no known workarounds.</p>
CSCse02543	<p>When some modems are in the reject state and a <b>clear cable modem reject delete</b> command is issued, a <code>CM_INCONSISTENCY</code> message is generated.</p> <p>Workaround: Do not use the <b>clear cable modem reject delete</b> command.</p>
CSCse04894	<p>Setting the lockout flag on the Working line card and then performing a <b>hw-module subslot x/y reset</b> of the line card causes a switchover from the Working to the Protect line card, disables the upconverter on the Active Protect line card, and causes all modems to go offline.</p> <p>There are no known workarounds.</p>
CSCse08252	<p>The cable modem termination subsystem (CMTS) receives a gate-set from Camiant DT tool, but it does not send gate-set-ack or gate-set-err, instead it creates the dynamic flow and the gate stays in auth mode.</p> <p>There are no known workarounds.</p>
CSCse22482	<p>After a Performance Routing Engine (PRE) failover, downstream voice traffic moves from dynamic flow to primary flow.</p> <p>There are no known workarounds.</p>
CSCse43344	<p>When a lockout of the Working card is followed by online insertion and removal (OIR), the following two problems occur: 1) OIR switches from the Working card to the Protect card, dropping all the cable modems. 2) After the Working card is back from the OIR, traffic stays on the Protect card with the cable modems down, and the Working card has lockout active. Clearing lockout fails, and because the Working card is standby, reverting to the Working card would also fail.</p> <p>There are no known workarounds.</p>
CSCse45342	<p>Configuring cable <code>default-tos-qos10 tos-overwrite</code> and resetting the modem does not create a new qos-profile. The modem comes online with the existing profile.</p> <p>The problem occurs on modems provisioned in Data-over-Cable Service Interface Specification (DOCSIS) 1.0 mode when the default <code>tos-mask</code> and <code>tos-value</code> are configured.</p> <p>There are no known workarounds.</p>

**Table 67** Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCse50735	<p>After a cable line card failover, the dynamic Service Flow (SF)-to-Multiprotocol Label Switching (MPLS) virtual private network (VPN) mapping feature no longer works.</p> <p>There are no known workarounds.</p>
CSCse54378	<p>On a Cisco uBR10000 series router running Cisco IOS image ubr10k-k9p6u2-mz.2006-06-02.123_17_BC, tracebacks are found at sch_rp_download_debug_info when you attempt to configure an already assigned address.</p> <p>There are no known workarounds.</p>
CSCse56676	<p>The cdrqCmtsCmRQDoneNotification trap, which indicates that the cable remote-query function has finished a polling cycle for modems on the cable modem termination system (CMTS), is sent to Simple Network Management Protocol (SNMP) management stations, even when cable specific traps are not configured to be sent to those stations.</p> <p>This condition occurs on a Cisco uBR series CMTS, and can occur on any trap sent, even when the trap is not associated with the SNMP host.</p> <p>There are no known workarounds.</p>
CSCse61661	<p>The dynamic flow is not mapped to the configured virtual routing and forwarding VRF instance if <b>cable dynamic-flow vrf name</b> is configured at the interface level. The mapping works correctly if <b>cable dynamic-flow vrf name</b> is configured globally. The configuration works correctly for a regular physical interface, but does not work on a bundle interface.</p> <p>There are no known workarounds.</p>
CSCse67808	<p>The cdpCacheTable contains entries with index 4294967295 that are only available using the Simple Network Management Protocol (SNMP) <b>get-next</b> command. When the <b>get-one</b> command is used to retrieve the same value, the NO_SUCH_INSTANCE_EXCEPTION is returned.</p> <p>This issue appears to be related to the management ethernet port on the secondary Performance Routing Engine (PRE) in a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCse67868	<p>The Simple Network Management Protocol (SNMP) cpmCPUTotalPhysicalIndex object returns valid entPhysicalIndex values for cable line cards when these values are retrieved using the <b>getnext</b> command, but when the <b>getone</b> command is used, the physical index values for the cable line cards (CLCs) are returned as 0.</p> <p>This issue occurs on Cisco uBR10000 series routers with cable line cards and SNMP configured.</p> <p>There are no known workarounds.</p>
CSCse69641	<p>When the <b>show cable modem s t</b> command is issued soon after a <b>clear cable modem all delete</b> command, the console and vty get stuck.</p> <p>The issue occurs in large-scale environments with more than 5000 modems.</p> <p>Workaround: Do not use the <b>clear cable modem all delete</b> command; delete specific modems instead.</p>

Table 67 Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCse78143	On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>show cr10k-rp cable x/y/z sid</b> command does not allow the service identifier (SID) value to be set to values greater than 8176. As a result, queues associated with downstream multicast quality of service (QoS) SIDs cannot be examined.  There are no known workarounds.
CSCse80641	The Transparent LAN Service (TLS) feature does not support stacked dot1q tags. This condition occurs when the TLS feature is configured, and the cable modem termination system (CMTS) receives a 1522 bytes packet (including the frame check sequence (FCS)) in the upstream direction that contains an 802.1q tag.  There are no known workarounds.
CSCse84566	This is a feature request for enhancing the Admission Control error messages to help analyze complex system test under heavy PC calls for long period of time.
CSCse86436	Massive Embedded Media Terminal Adapter (eMTA) flapping occurs after long hours of more than 1000 PacketCable Multimedia (PCMM) calls. All flapping eMTAs re-register back.  There are no known workarounds.
CSCse86458	Many Arris Embedded Media Terminal Adapters (eMTAs) on an Asynchronous Time Division Multiple Access (ATDMA) channel go offline after an MC520u CLI switchover with PacketCable calls.  There are no known workarounds.
CSCse86778	The <b>show cable spectrum-group x</b> output is not synchronized in the standby Performance Routing Engine (PRE).
CSCse88149	The <b>show cable admission-control interface</b> command does not display a DS service class name that has been configured using the <b>cable admission-control us-bandwidth service-class</b> command. The original command was accepted without any error message, and the configuration is seen in the running configuration.  There are no known workarounds.
CSCse88914	The total of exclusive bandwidth allocated to various service class names of a particular scheduling type exceeds the exclusive allocation configured for that scheduling type.  There are no known workarounds.
CSCse97919	After the first Performance Routing Engine (PRE) switchover from the active PRE to the standby PRE, the link LED on the PRE stops working.  There are no known workarounds.
CSCsf02982	When an attempt is made to modify the in-use Peer-to-Peer (P2P) policy, an error occurs.  There are no known workarounds.

**Table 67**      **Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)**

DDTS ID Number	Description
CSCsf04338	<p>The Cisco uBR series cable modem termination system (CMTS) with cable or bundle subinterfaces configured does not prevent customer premises equipment (CPE) from receiving a Dynamic Host Configuration Protocol (DHCP) offer with an IP address belonging to the wrong subinterface. Only DHCP offers that contain an offered IP address within the same subinterface as the cable modem belonging to the customer premises equipment (CPE) should be forwarded by the CMTS.</p> <p>The issue occurs when the CMTS is configured to use cable or bundle subinterfaces and the DHCP server is misconfigured.</p> <p>Workaround: Ensure that the DHCP server is configured to assign CPE devices IP addresses from only the appropriate IP subnets.</p>
CSCsf30877	<p>The wrong classification is applied to the IP Protocol field.</p> <p>There are no known workarounds.</p>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>
CSCsg08747	<p>When IPsec is enabled on the cable modem termination system (CMTS) network interface, but not enabled on the associated PC, a ping from the PC to the CMTS gets an unexpected response.</p> <p>This issue occurs because the security association is enabled on one side and not the other. The expected behavior would be that a ping should fail, but the CMTS replies.</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsg17050	<p>The DOCSIS Set-Top Gateway (DSG) interface configuration is not retained when a 5X20S card is replaced with a 5x20U card, and vice versa.</p> <p>Workaround: Remove the <b>dsg tg</b> configuration from the global configuration, configure it again, and apply the configuration to the interface.</p>
CSCsg41805	<p>A cable modem is not pingable after a reset modem from the cable modem termination system (CMTS). The cable modem gets stuck in the init(d) state and is not able to come online.</p> <p>This issue occurs in Hot Standby Connection-to-Connection Protocol (HCCP) line card redundancy and virtual interface (VI) bundle interface configurations and can occur on the Protect line card after different line card failovers and Route Processor switchovers.</p> <p>Workaround: Failover back to the Working line card.</p>

Table 67 Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsg44938	<p>On a Cisco uBR10000 series router running an interface-level Hot Standby Connection-to-Connection Protocol (HCCP) configuration, a swap between the MC520H card and MC520u card forces the first JIB's downstreams into the shutdown state. For instance, if you downgrade from the MC520H card to the MC520u card, notice that the MC520u card shut down Cx/y/0 and Cx/y/2 during the building of its configuration.</p> <p>This issue occurs when the Cisco uBR10000 series router is running Cisco IOS Release 12.3(17a)BC2 with an HCCP Interface-Level configuration and <b>cr10k card slot/subslot oir-compatibility</b> is enabled.</p> <p>Workaround: 1. Enter <b>no shut</b> on the affected interfaces before doing an HCCP revertback, or 2. Remove the interface-level HCCP configuration and replace it with a global HCCP configuration.</p>
CSCsg49060	<p>A portion of the modems become unpingable even though they are in the online(pt) state following a Hot Standby Connection-to-Connection Protocol (HCCP) failover.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC2 with a global HCCP configuration.</p> <p>Workaround: Reset each unpingable cable modem (CM), and the CM will return to a working state.</p>
CSCsg55917	<p>After an upgrade of the cable modem termination system (CMTS) to Cisco IOS Release 12.3(17a)BC2 and a reload, some cable modems get stuck in the reject(na) state.</p> <p>There are no known workarounds.</p>
CSCsg59620	<p>The following errors are generated after Usage Based Billing/SAMIS (cable metering) is enabled on a Cisco uBR10012 router running Cisco IOS Release 12.3(17a)BC2:</p> <pre>SLOT x/y: Oct x hh:mm:ss: %AMDP2_FE-6-EXCESSCOLL: FastEthernet1/0 TDR=0, TRC=0</pre> <p>There is no known adverse affect on the operation of the router.</p> <p>There are no known workarounds other than disabling the Subscriber Account Management Interface Specification (SAMIS) feature.</p>
CSCsg67014	<p>The <b>show cable modem vendor summary</b> command output displays SB4100 cable modems that are in the reject(pk) state as "registered," which is misleading.</p> <p>The "Oper" column in the <b>show cable modem summary</b> output should be added to the <b>show cable modem vendor summary</b> and <b>show cable modem vendor summary total</b> outputs.</p> <p>There are no known workarounds</p>
CSCsg70266	<p>The <b>show int bundle</b> counter does not display correctly after a line card (LC) is switched over to the Protect LC. The counter is not correct again until the line card reverts back to the Working LC.</p> <p>There are no known workarounds</p>

**Table 67**      **Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)**

DDTS ID Number	Description
CSCsg75417	<p>On an MC520u card, signal-to-noise ratio (SNR) values might drop on an upstream, which could cause modems to drop offline.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC3 with multiple MC520u cards configured for pre-equalization.</p> <p>Workaround: 1. Disable/enable pre-equalization on the upstream. 2. Change the minislot size.</p>
CSCsg80690	<p>When reverting from a Protect U card to a Working H card, most cable modems on 6.4MHz ATDMA DOC 2.0 channels drop offline. Other upstream channels work correctly.</p> <p>This issue typically occurs in 50% of the reverts performed.</p> <p>There are no known workarounds other than to not use 6.4MHz ADMTA channels.</p>
CSCsg80760	<p>Cable modems are becoming unpingable within minutes of registration. The modems are still online and DOCSIS pings are successful. Signal-to-noise ratio (SNR) is between around 17dB for 64QAM and 6.4 Mhz channel width.</p> <p>The issue exists on only one upstream at a time. Moving modems from the upstream to another cable line card (CLC) and then back causes the issue to reappear on the same or different upstream. The problem seems to occur only on a 1x8 MAC domain with modems on all 8 upstreams.</p> <p>Workaround: Remove pre-equalization, and reset the CLC.</p>
CSCsg82102	<p>A Cisco uBR10000 series running Cisco IOS Release 12.3(17a)BC2 with a Subscriber Account Management Interface Specification (SAMIS) cable-monitor, may not stream online cable modems.</p> <p>There are no known workarounds</p>
CSCsg82987	<p>The Simple Network Management Protocol (SNMP) output counters for downstream interfaces and input counters for upstream interfaces are missing for the MC520u0-d card.</p> <p>This issue occurs on a Cisco uBR10000 series router (PRE2-RP) running Cisco IOS Release 12.3(17a)BC2 or 12.3(17a)BC1.</p> <p>There are no known workarounds.</p>
CSCsg87381	<p>When Internetwork Packet Exchange (IPX) packets are sent to a bundle interface, the ifInUnknownPkts counter value remains "0."</p> <p>There are no known workarounds.</p>
CSCsh05436	<p>Service flows are refused because downstream latency cannot be met by the card.</p> <p>This issue occurs on interfaces having a negative value in the worst case latency for low latency queue, and is caused by using a noncompliant packetcable setup with the packetcable vanilla command. The <b>packetcable authorize vanilla-docsis-mta</b> command allows the receipt of non-compliant service flows. The issue does not occur in a compliant packetcable setup because the "Downstream Latency" value is not permitted.</p> <p>Workaround: Reset the card.</p>

Table 67 Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsh11414	<p>A Cisco UBR10000 series router running Cisco IOS Release 12.3(17a)BC2 and configured for Subscriber Account Management Interface Specification (SAMIS) does not save deleted service flows for an offline cable modem if the <b>cable primary-sflow-qos11 keep all</b> command is configured. Consequently, the deleted service flows are absent from the SAMIS and the docsQosServiceFlowLogTable.</p> <p>Workaround: Remove the <b>cable primary-sflow-qos11 keep all</b> command to save the deleted service flow information.</p>
CSCsh19917	<p>Some parent warnings appear when static analysis is performed on the specmib source file.</p> <p>Workaround: No workaround is required. The functionality of the MIB query is not affected.</p>
CSCsh20158	<p>On a Cisco uBR series cable modem termination system (CMTS), if the <b>cable source-verify dhcp</b> function receives a NAK in response to a Dynamic Host Configuration Protocol (DHCP) leasequery, it stops sending any more leasequeries until the system performs a successful DHCP release/renew.</p> <p>This issue could potentially stop a legitimate user from getting connectivity for a short period of time.</p> <p>There are no known workarounds.</p>
CSCsh24410	<p>After upgrading to Cisco IOS Release 12.3(17b)BC4, some sites report their speed is down.</p> <p>No buffer counters are increased when the <b>show interface command</b> is executed.</p> <p>There are no known workarounds.</p>
CSCsh24533	<p>The router-id for Open Shortest Path First (OSPF) is not getting synchronized in the standby Performance Routing Engine (PRE).</p> <p>Workaround: After PRE switch over, reconfigure a router-id to OSPF.</p>
CSCsh33283	<p>The following error is reported, shortly after a hardware swap:</p> <pre>%Software-forced reload Unexpected exception, CPU signal 23, PC = 0x6013EF0C -Traceback= 6013EF0C 6013CEC0</pre> <p>There are no known workarounds.</p>
CSCsh38866	<p>When the bundle interface is unconfigured and both the interface and the default interface are shut down at the same time, the interface shows both the active and standby Route Processor (RP) in Inconsistent states.</p> <p>There are no known workarounds.</p>

**Table 67** Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsh39260	<p>The following inconsistent Internet Control Message Protocol (ICMP) unreachable behaviors occur between a Cisco uBR7200VXR router and a Cisco uBR10000 series router when cable filters are applied.</p> <ol style="list-style-type: none"> <li>1. The Cisco uBR10000 series router sends an ICMP type 13 code 3 (Communication Administratively Prohibited) regardless of configuration of "no ip unreachable" under bundle interface when a packet violates an active upstream (US) cable filter.</li> <li>2. The Cisco uBR7200VXR router never sends an ICMP type 13 code 3 regardless of configuration of "ip unreachable" under bundle interface when a packet violates an active US cable filter.</li> </ol> <p>Both the cable modem and customer premises cable filter groups exhibit this behavior.</p> <p>There are no known workarounds.</p>
CSCsh40234	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC6, reports the following message with traceback in the log of the active PRE1 for many different cable modems:</p> <pre>Jan 10 10:29:26 EST: %UBR10000-3-INVALIDSIDPOSITION: Invalid SID (2166) position for interface Cable5/0/0: CM 0011.e358.5d05:Is used by CM 0090.649d.2795 SFID 3679 SID 1834.SID container info: start 8170 end 5766</pre> <p>There are no known workarounds.</p>
CSCsh40309	<p>The burst is not being displayed during a modem upstream (US) trace with Cisco Broadband Troubleshooter (CBT) Version 3.2 when pre-equalization is configured on the US port.</p> <p>This issue occurs only on the 5x20S and U cards when pre-equalization (equalization-coefficient) is configured.</p> <p>This issue doesn't seem to occur on the 28U cards, so it may not be prevalent on the 5x20H either because that card also uses Broadcom for the upstream (US) chip. The TI4522 chip is used on the 5x20S and U cards.</p> <p>Workaround: Do not configure the pre-equalization feature. Note that this feature is off by default.</p>
CSCsh40400	<p>Lower throughput rates occur when the default upstream (US) setting of "token bucket rate limiting with shaping" is enabled.</p> <p>This issue seems to occur because the shaping is causing the rate limiting to kick in too early, resulting in premature delayed grants, and reduced bandwidth.</p> <p>Workaround: Disable shaping and only use token bucket rate limiting if you want to achieve high throughputs in the US.</p>
CSCsh41508	<p>The PacketCable Multimedia (PCMM) time-based-usage timer is not sending gate-report-state at expected time.</p> <p>There are no known workarounds.</p>
CSCsh44794	<p>In the subtract_spectrum_band function, the wrong codes are used to swap the lowband_bound and upper_band.</p> <p>There are no known workarounds.</p>

**Table 67** Open Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsh50221	<p>The MC5x20 line card crashes on a Cisco uBR10000 series router IOS running Cisco IOS Release 12.3(13a)BC6 because of a bus error exception.</p> <p>There are no known workarounds.</p>
CSCsh52141	<p>When a Common Open Policy Service (COPS) session is initiated by a call agent (COPS server), the cable modem termination system (CMTS) is supposed to use the Differentiated Services Code Point (DSCP) value of the call agent that started the session.</p> <p>However, when a call agent (COPS server) opens a Transmission Control Protocol (TCP) session to the CMTS over the well known PacketCable COPS TCP port 2126 with a DSCP value of CS3 (IP TOS 3), the CMTS uses a DSCP value of 0 (IP TOS 0). Improper or unexpected type-of-service (ToS) values can lead to unpredictable quality of service (QoS) issues elsewhere in the network.</p> <p>Workaround: Manually configure the DSCP value for the COPS session on the CMTS using the <b>cops ip dscp x</b> configuration command.</p>

## Resolved Caveats for Release 12.3(17b)BC5

[Table 68](#) lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC5..

**Table 68**      **Resolved Caveats for Cisco IOS Release 12.3(17b)BC5**

DDTS ID Number	Description
CSCsb12598	<p data-bbox="613 310 1528 436">Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.</p> <p data-bbox="613 457 1528 611">Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.</p> <p data-bbox="613 632 1219 657">Cisco IOS is affected by the following vulnerabilities:</p> <p data-bbox="613 678 1474 703">Processing ClientHello messages, documented as Cisco bug ID CSCsb12598</p> <p data-bbox="613 724 1403 779">Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304</p> <p data-bbox="613 800 1438 825">Processing Finished messages, documented as Cisco bug ID CSCsd92405</p> <p data-bbox="613 846 1516 930">Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.</p> <p data-bbox="613 951 1520 1035">This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL</a></p> <hr/> <p data-bbox="613 1056 1520 1297"><b>Note</b>  Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto</a></p> <hr/> <p data-bbox="613 1339 1516 1453">A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: <a href="http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml</a>.</p>

Table 68 Resolved Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsb40304	<p>Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.</p> <p>Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.</p> <p>Cisco IOS is affected by the following vulnerabilities:</p> <p>Processing ClientHello messages, documented as Cisco bug ID CSCsb12598</p> <p>Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304</p> <p>Processing Finished messages, documented as Cisco bug ID CSCsd92405</p> <p>Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.</p> <p>This advisory is posted at  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL</a></p> <p>Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto</a></p> <p>A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:  <a href="http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml</a></p>
CSCsc72722	<p>Transmission Control Protocol (TCP) connections that are opened through a Cisco IOS Firewall (Context-Based Access Control (CBAC)) do not timeout.</p> <p>This issue occurs when the Cisco IOS Firewall (CBAC) is enabled because the TCP idle timer for a session can be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This situation can lead to the TCP session not timing out.</p> <p>There are no known workarounds.</p>
CSCsd33394	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), upstream subscriber traffic management filters do not filter packets with a multicast destination IP address.</p> <p>Workaround: Configure and apply an ip access-list to the cable or bundle interface. This configuration will apply to traffic from all modems and CPE on the interface.</p>

**Table 68 Resolved Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)**

DDTS ID Number	Description
CSCsd92405	<p data-bbox="613 310 1528 436">Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.</p> <p data-bbox="613 457 1528 615">Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.</p> <p data-bbox="613 636 1528 657">Cisco IOS is affected by the following vulnerabilities:</p> <p data-bbox="613 678 1528 699">Processing ClientHello messages, documented as Cisco bug ID CSCsb12598</p> <p data-bbox="613 720 1528 783">Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304</p> <p data-bbox="613 804 1528 825">Processing Finished messages, documented as Cisco bug ID CSCsd92405</p> <p data-bbox="613 846 1528 930">Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.</p> <p data-bbox="613 951 1528 1035">This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL</a></p> <hr/> <p data-bbox="613 1056 1528 1098"> <b>Note</b> Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:</p> <p data-bbox="703 1234 1528 1297"><a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto</a></p> <hr/> <p data-bbox="613 1339 1528 1455">A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: <a href="http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml</a>.</p>
CSCse71725	<p data-bbox="613 1476 1528 1560">The <b>cable monitor</b> command does not successfully monitor upstream bandwidth request messages on a Cisco uBR10000 series cable modem termination system (CMTS).</p> <p data-bbox="613 1581 1528 1612">There are no known workarounds.</p>
CSCse82337	<p data-bbox="613 1623 1528 1686">An onboard FastEthernet board (interface fastethernet 0/0/0) cannot recognize that the line protocol is down.</p> <p data-bbox="613 1707 1528 1728">This issue occurs immediately after reloading the PRE-2.</p> <p data-bbox="613 1749 1528 1772">Workaround: Perform a <b>shut/no shut</b> of the interface, or reload the PRE-2 again.</p>

Table 68 Resolved Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsf07847	<p>Specifically crafted Cisco Discovery Protocol (CDP) packets can cause a router to allocate and keep extra memory. Exploitation of this behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router. Since CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.</p> <p>This issue can occur when the CDP packet header length is lesser than predefined header length (4 bytes).</p> <p>Workaround: Disable CDP on interfaces where it is not necessary.</p>
CSCsf19110	<p>Tracebacks and memory allocation failure messages occur in the MC520u cards.</p> <p>This issue occurs in a large scale setup of more than 5000 modems, when you copy a baseline privacy interface (BPI)-enabled configuration file and then enter a <b>clear cable modem all del</b> command. The errors occur after more than 4000 modems are up.</p> <p>There are no known workarounds.</p>
CSCsf28437	<p>The exec-timeout value for line vty doesn't synchronize with the standby Performance Routing Engine (PRE) after a <b>write memory</b> command is executed. The value of the exec-timeout is overwritten to "0". The startup-configuration on both PREs is overwritten correctly.</p> <p>This issue occurs when PRE redundancy is configured on a Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC2 or 12.3(17a)BC2.</p> <p>Workaround: Reconfigure the exec-timeout under the line vty, or reload the PRE.</p>
CSCsf96635	<p>Traceback and the following error message are reported by the router after a period of normal operation:</p> <pre>%GENERAL-3-EREVENT: HWCEF: Loadinfo fastadj lock with NULL fasttag_rew</pre> <p>There are no known workarounds.</p>
CSCsg13635	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), a manual Hot Standby Connection-to-Connection Protocol (HCCP) N+1 line card switchover fails if one cable interface on the line card being switched over is shutdown. An error message similar to the following is reported:</p> <pre>% HCCP 2 60: aborts switchover. Request later.</pre> <p>The issue seems to occur when the individual cable interface was in the shutdown state when the CMTS was activated. The issue does not seem to occur if the cable interface was shutdown after the CMTS has been operational.</p> <p>Workaround: Activate the shutdown cable interface with the <b>no shutdown</b> cable interface command. Optionally, add the <b>no keepalive</b> cable interface command if no cable modems are expected to be online on the interface.</p>

**Table 68** Resolved Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsg16908	<p>Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.</p> <p>The Cisco IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS FTP Server service are unaffected by these vulnerabilities.</p> <p>This vulnerability does not apply to the Cisco IOS FTP Client feature.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070509-iosftp">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070509-iosftp</a></p>
CSCsg25988	<p>In a Performance Routing Engine (PRE) and line card redundancy configuration, the following Hot Standby Connection-to-Connection Protocol (HCCP) failure can occur:</p> <pre data-bbox="613 871 1528 919">Active RP, %HCCP-5-FAILURE: Grp x Mbr y Protect: received failure notice-keepalive failure.</pre> <p>This issue occurs in a global line card redundancy configuration after a line card failover and PRE switchover. The Protect line card may fall back to the Working line card if the Protect line card has keepalive failure configured.</p> <p>There are no known workarounds.</p>
CSCsg36536	<p>A partial line card switchover occurs in a bundled virtual interface (VI) configuration. Some of the Protect line cards of downstream ports are in the standby state and some are in active state.</p> <p>There are no known workarounds.</p>
CSCsg39990	<p>Cable filter groups do not filter local traffic on the Cisco uBR10000 series platform.</p> <p>There are no known workarounds.</p>
CSCsg41840	<p>A cable modem termination system (CMTS) line card crash occurs when the <b>show cable modem cable x/y error</b> command is issued.</p> <p>Workaround: Do not issue the <b>show cable modem cable x/y error</b> command while logging into the line card.</p>
CSCsg57108	<p>A Protect line card crash occurs when the <b>default interface c/x/y/c</b> command is issued immediately after Hot Standby Connection-to-Connection Protocol (HCCP) synchronization.</p> <p>There are no known workarounds.</p>

Table 68 Resolved Caveats for Cisco IOS Release 12.3(17b)BC5 (continued)

DDTS ID Number	Description
CSCsg70355	<p>Starting in calendar year 2007, daylight savings summer-time rules may cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.</p> <p>The issue occurs because the Cisco IOS <b>clock summer-time zone recurring</b> configuration command uses the United States standards for daylight savings time rules by default. The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March. It changes the end date from the last Sunday of October to the first Sunday of November.</p> <p>Workaround: Use the <b>clock summer-time</b> configuration command to manually configure the proper start date and end date for daylight savings time.</p> <p>Note that using Network Time Protocol (NTP) is not a workaround to this problem. NTP does not carry any information about time zones or summertime.</p>
CSCsg90384	<p>Cable filter-groups do not filter based on type-of-service (ToS) value except when the <b>mask</b> "0x0" and <b>tos</b> "0x0" values are used.</p> <p>The CMTS_PKT_FILTER_GROUP_x access-list built by the filter group always contains the following statement irrespective of the <b>mask</b> and <b>tos</b> values entered under the <b>cable filter-group</b> command except when the <b>mask</b> "0x0" and <b>tos</b> "0x0" values are used:</p> <pre data-bbox="574 999 1474 1125">10K#sh access-list CMTS_PKT_FILTER_GROUP_2 Load for five secs: 5%/2%; one minute: 5%; five minutes: 5% Time source is NTP, 18:38:52.458 PST Wed Nov 29 2006 Extended IP access list CMTS_PKT_FILTER_GROUP_2 (per-user) (Compiled) (PXF security) (snip) deny ip any any precedence routine (snip)</pre> <p>When the <b>mask</b> "0x0" and <b>tos</b> "0x0" values are used, the access-list statement changes to <b>deny ip any any</b>, which is the proper behavior defined by the DOCSIS OSSI specification. Other filter parameters, such <b>src/dest ip</b> or <b>src/dest tcp/udp port #</b>, work correctly.</p> <p>There are no known workarounds.</p>
CSCsh06777	<p>The cable filter group assigned to the cable modem is not applied. Instead, the filter group of the customer premises equipment (CPE) is applied instead.</p> <p>There are no known workarounds.</p>
CSCsh12789	<p>Mixing Quadrature Amplitude Modulation 16 (QAM16) and Quadrature Amplitude Modulation 16 (QAM16) for IM and SM on the 5x20H card prevents cable modems from getting past init(r1) on 5x20H card. This problem does not occur on U or S cards.</p> <p>Workaround: Configure QAM16 or QPSK for both IM an SM.</p>

DDTS ID Number	Description
CSCsb12598	<p data-bbox="613 260 1529 386">Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.</p> <p data-bbox="613 407 1529 562">Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.</p> <p data-bbox="613 575 1218 604">Cisco IOS is affected by the following vulnerabilities:</p> <p data-bbox="613 621 1474 651">Processing ClientHello messages, documented as Cisco bug ID CSCsb12598</p> <p data-bbox="613 667 1403 726">Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304</p> <p data-bbox="613 743 1438 772">Processing Finished messages, documented as Cisco bug ID CSCsd92405</p> <p data-bbox="613 789 1516 877">Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.</p> <p data-bbox="613 894 1520 987">This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL</a></p> <hr/> <p data-bbox="613 1008 662 1045"></p> <p data-bbox="613 1054 1516 1239"><b>Note</b> Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto</a></p> <hr/> <p data-bbox="613 1281 1516 1400">A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: <a href="http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml</a>.</p>

DDTS ID Number	Description
CSCsb40304	<p>Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.</p> <p>Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.</p> <p>Cisco IOS is affected by the following vulnerabilities:</p> <p>Processing ClientHello messages, documented as Cisco bug ID CSCsb12598</p> <p>Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304</p> <p>Processing Finished messages, documented as Cisco bug ID CSCsd92405</p> <p>Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.</p> <p>This advisory is posted  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL</a>.</p> <hr/> <p> <b>Note</b> Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto</a></p> <hr/> <p>A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:  <a href="http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml</a>.</p>
CSCsc72722	<p>Transmission Control Protocol (TCP) connections that are opened through a Cisco IOS Firewall (Context-Based Access Control (CBAC)) do not timeout.</p> <p>This issue occurs when the Cisco IOS Firewall (CBAC) is enabled because the TCP idle timer for a session can be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This situation can lead to the TCP session not timing out.</p> <p>There are no known workarounds.</p>
CSCsd33394	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), upstream subscriber traffic management filters do not filter packets with a multicast destination IP address.</p> <p>Workaround: Configure and apply an ip access-list to the cable or bundle interface. This configuration will apply to traffic from all modems and CPE on the interface.</p>

DDTS ID Number	Description
CSCsd92405	<p>Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.</p> <p>Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.</p> <p>Cisco IOS is affected by the following vulnerabilities:</p> <p>Processing ClientHello messages, documented as Cisco bug ID CSCsb12598</p> <p>Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304</p> <p>Processing Finished messages, documented as Cisco bug ID CSCsd92405</p> <p>Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.</p> <p>This advisory is posted at  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL</a></p> <hr/> <p> <b>Note</b> Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto</a></p> <hr/> <p>A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:  <a href="http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml</a>.</p>
CSCse71725	<p>The <b>cable monitor</b> command does not successfully monitor upstream bandwidth request messages on a Cisco uBR10000 series cable modem termination system (CMTS).</p> <p>There are no known workarounds.</p>
CSCse82337	<p>An onboard FastEthernet board (interface fastethernet 0/0/0) cannot recognize that the line protocol is down.</p> <p>This issue occurs immediately after reloading the PRE-2.</p> <p>Workaround: Perform a <b>shut/no shut</b> of the interface, or reload the PRE-2 again.</p>

DDTS ID Number	Description
CSCsf07847	<p>Specifically crafted Cisco Discovery Protocol (CDP) packets can cause a router to allocate and keep extra memory. Exploitation of this behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router. Since CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.</p> <p>This issue can occur when the CDP packet header length is lesser than predefined header length (4 bytes).</p> <p>Workaround: Disable CDP on interfaces where it is not necessary.</p>
CSCsf19110	<p>Tracebacks and memory allocation failure messages occur in the MC520u cards.</p> <p>This issue occurs in a large scale setup of more than 5000 modems, when you copy a baseline privacy interface (BPI)-enabled configuration file and then enter a <b>clear cable modem all del</b> command. The errors occur after more than 4000 modems are up.</p> <p>There are no known workarounds.</p>
CSCsf28437	<p>The exec-timeout value for line vty doesn't synchronize with the standby Performance Routing Engine (PRE) after a <b>write memory</b> command is executed. The value of the exec-timeout is overwritten to "0". The startup-configuration on both PREs is overwritten correctly.</p> <p>This issue occurs when PRE redundancy is configured on a Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC2 or 12.3(17a)BC2.</p> <p>Workaround: Reconfigure the exec-timeout under the line vty, or reload the PRE.</p>
CSCsf96635	<p>Traceback and the following error message are reported by the router after a period of normal operation:</p> <pre>%GENERAL-3-EREVENT: HWCEF: Loadinfo fastadj lock with NULL fasttag_rew</pre> <p>There are no known workarounds.</p>
CSCsg13635	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), a manual Hot Standby Connection-to-Connection Protocol (HCCP) N+1 line card switchover fails if one cable interface on the line card being switched over is shutdown. An error message similar to the following is reported:</p> <pre>% HCCP 2 60: aborts switchover. Request later.</pre> <p>The issue seems to occur when the individual cable interface was in the shutdown state when the CMTS was activated. The issue does not seem to occur if the cable interface was shutdown after the CMTS has been operational.</p> <p>Workaround: Activate the shutdown cable interface with the <b>no shutdown</b> cable interface command. Optionally, add the <b>no keepalive</b> cable interface command if no cable modems are expected to be online on the interface.</p>

DDTS ID Number	Description
CSCsg16908	<p>Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.</p> <p>The Cisco IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS FTP Server service are unaffected by these vulnerabilities.</p> <p>This vulnerability does not apply to the Cisco IOS FTP Client feature.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070509-iosftp">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070509-iosftp</a></p>
CSCsg25988	<p>In a Performance Routing Engine (PRE) and line card redundancy configuration, the following Hot Standby Connection-to-Connection Protocol (HCCP) failure can occur:</p> <pre>Active RP, %HCCP-5-FAILURE: Grp x Mbr y Protect: received failure notice-keepalive failure.</pre> <p>This issue occurs in a global line card redundancy configuration after a line card failover and PRE switchover. The Protect line card may fall back to the Working line card if the Protect line card has keepalive failure configured.</p> <p>There are no known workarounds.</p>
CSCsg36536	<p>A partial line card switchover occurs in a bundled virtual interface (VI) configuration. Some of the Protect line cards of downstream ports are in the standby state and some are in active state.</p> <p>There are no known workarounds.</p>
CSCsg39990	<p>Cable filter groups do not filter local traffic on the Cisco uBR10000 series platform.</p> <p>There are no known workarounds.</p>
CSCsg41840	<p>A cable modem termination system (CMTS) line card crash occurs when the <b>show cable modem cable x/y error</b> command is issued.</p> <p>Workaround: Do not issue the <b>show cable modem cable x/y error</b> command while logging into the line card.</p>
CSCsg57108	<p>A Protect line card crash occurs when the <b>default interface c x/y/c</b> command is issued immediately after Hot Standby Connection-to-Connection Protocol (HCCP) synchronization.</p> <p>There are no known workarounds.</p>

DDTS ID Number	Description
CSCsg70355	<p>Starting in calendar year 2007, daylight savings summer-time rules may cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.</p> <p>The issue occurs because the Cisco IOS <b>clock summer-time zone recurring</b> configuration command uses the United States standards for daylight savings time rules by default. The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March. It changes the end date from the last Sunday of October to the first Sunday of November.</p> <p>Workaround: Use the <b>clock summer-time</b> configuration command to manually configure the proper start date and end date for daylight savings time.</p> <p>Note that using Network Time Protocol (NTP) is not a workaround to this problem. NTP does not carry any information about time zones or summertime.</p>
CSCsg90384	<p>Cable filter-groups do not filter based on type-of-service (ToS) value except when the <b>mask</b> "0x0" and <b>tos</b> "0x0" values are used.</p> <p>The CMTS_PKT_FILTER_GROUP_x access-list built by the filter group always contains the following statement irrespective of the <b>mask</b> and <b>tos</b> values entered under the <b>cable filter-group</b> command except when the <b>mask</b> "0x0" and <b>tos</b> "0x0" values are used:</p> <pre data-bbox="574 951 1474 1077">10K#sh access-list CMTS_PKT_FILTER_GROUP_2 Load for five secs: 5%/2%; one minute: 5%; five minutes: 5% Time source is NTP, 18:38:52.458 PST Wed Nov 29 2006 Extended IP access list CMTS_PKT_FILTER_GROUP_2 (per-user) (Compiled) (PXF security) (snip) deny ip any any precedence routine (snip)</pre> <p>When the <b>mask</b> "0x0" and <b>tos</b> "0x0" values are used, the access-list statement changes to <b>deny ip any any</b>, which is the proper behavior defined by the DOCSIS OSSI specification. Other filter parameters, such <b>src/dest ip</b> or <b>src/dest tcp/udp port #</b>, work correctly.</p> <p>There are no known workarounds.</p>
CSCsh06777	<p>The cable filter group assigned to the cable modem is not applied. Instead, the filter group of the customer premises equipment (CPE) is applied instead.</p> <p>There are no known workarounds.</p>
CSCsh12789	<p>Mixing Quadrature Amplitude Modulation 16 (QAM16) and Quadrature Amplitude Modulation 16 (QAM16) for IM and SM on the 5x20H card prevents cable modems from getting past init(r1) on 5x20H card. This problem does not occur on U or S cards.</p> <p>Workaround: Configure QAM16 or QPSK for both IM an SM.</p>

## Open Caveats for Release 12.3(17b)BC4

Table 69 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC4.

**Table 69** Open Caveats for Cisco IOS Release 12.3(17b)BC4

DDTS ID Number	Description
CSCef66578	<p>The output of the <b>show cable modem connectivity</b> command displays an extremely large value.</p> <p>This issue occurs in Cisco IOS Releases 12.2(15)BC2b and 12.2(15)BC2c.</p> <p>There are no known workarounds.</p>
CSCeg30757	<p>A standby Performance Routing Engine (PRE) reloads unexpectedly. There is no impact on the primary PRE, and the router continues to function as normal.</p> <p>This issue occurs only when a Hot Standby Connection-to-Connection Protocol (HCCP) switchover is enabled through the command line interface on the router.</p> <p>Workaround: There are no known workarounds, other than to avoid enabling the HCCP switchover.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>
CSCej52423	<p>The wrong number of bytes are suppressed and packet drops occur on the dial shelf controller (DSC) when adding payload header suppression (PHS) and line card (LC) switchover.</p> <p>This issue occurs when performing a switchover while using LC redundancy and Multiple PHS for a secondary service flow (SF).</p> <p>Workaround: Do not use PHS with multiple rules for an SF if you are using N+1.</p>
CSCek21720	<p>Traceback occurs with packet intercept during a line card (LC) switchover in PRE2.</p> <p>This issue occurs when the LC switchover is performed while PacketCable (PC) calls and class features are in progress.</p> <p>There are no known workarounds</p>

**Table 69 Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

DDTS ID Number	Description
CSCek23320	<p>Simple Network Management Protocol (SNMP)-related traceback occurs when the image is loaded with the attached cable modem termination system (CMTS) configuration:</p> <pre>*Dec 21 16:11:28.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/1, changed state to up Dec 21 16:12:08.141: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61156234 reading 0x0 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 61156234 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 6115623C 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:14:11.138: %AAAA-3-DROPACCTSNDFAIL: Accounting record dropped, send to server failed: system-start</pre> <p>There are no known workarounds.</p>
CSCek24075	<p>Zero nodes are reported in the <b>show srp topology</b> command.</p> <p>There are no known workarounds.</p>
CSCek27678	<p>The <b>show access-list</b> command displays the access control lists (ACLs) for deleted packet filter groups. The corresponding internal ACLs are not removed, even after the packet filter group is deleted.</p> <p>The <b>show cable filter</b> command lists the reserved ACL group 255 index 1 with drop action, even if all the cable filter configurations have been removed from the cable modem termination system (CMTS).</p> <p>There are no known workarounds.</p>
CSCek31526	<p>The Inter-Process Communication (IPC) between cable CLCs occasionally fails.</p> <p>Workaround: Reload the image to fix this issue.</p>
CSCek34311	<p>The Performance Routing Engine (PRE) unexpectedly reloads if the <b>cable upstream n frequency up-freq-hz</b> command is repeated more than 500 times.</p> <p>There are no known workarounds.</p>
CSCek35970	<p>The IP ToS/DSCP byte is not overwritten for PacketCable CALEA replicated packets with the value received by GATE-SET COPS messages.</p> <p>There are no known workarounds.</p>
CSCek37518	<p>Client information is not displayed in the <b>show cable dsx tunnel ?</b> command when the tunnel group is not associated with a downstream interface.</p> <p>There are no known workarounds.</p>
CSCek38598	<p>No corresponding parallel express forwarding (PXF) queue is created for the new dynamic service flow when testing the dynamic service messaging (DSX) with the <b>test cable DSA</b> command.</p> <p>The real Media Terminal Adapters (MTAs) are able to make call with DSX without any problem.</p> <p>There are no known workarounds.</p>
CSCek39428	<p>DC Directory (DCD) messages do not get captured if the <i>mac-address</i> parameter is specified in the <b>cable monitor</b> command.</p> <p>There are no known workarounds.</p>

**Table 69**      **Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

DDTS ID Number	Description
CSCek42764	<p>After an LC switchover, the working standby interface configuration is displayed in the <b>show dsgr tunnel</b> output.</p> <p>Workaround: Skip the standby interface when scanning cable interfaces to display the DOCSIS Set-Top Gateway (DSG) tunnel information.</p>
CSCek48531	<p>A miscreant user alters the MAC address of their cable modem to match the MAC address of another cable modem on the same cable modem termination system (CMTS) chassis in an attempt to steal service by impersonating the legitimate user. Instead, the legitimate user is taken offline constantly, and neither modem stays online for more than 10-30 seconds. CMTS logs show a CM_MOVED message each time the modem moves from port to port. CMTS logs may show a Spoof or bad QoS registration message if the modem is on the same port, or may not show any logs.</p> <p>This condition can occur when the modem is one of several cable modem models susceptible to this modification. These models represent about 1/3 of all cable modems deployed worldwide.</p> <p>Workaround: There are no known workarounds other than to replace the legitimate user's cable modem with a new one. The legitimate user is always taken offline.</p>
CSCek59655	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC6 reloads in the production environment</p> <p>There are no known workarounds.</p>
CSCin98031	<p>N+1 synchronization does not occur when switching over from the Working card to the Protect card.</p> <p>There are no known workarounds.</p>
CSCsa53610	<p>The router fails to come up in Route Processor Redundancy (RPR) mode.</p> <p>This condition is caused by the fix for CSCef64718, which moved around the time point of posting PEER_COMM loss at switchover.</p> <p>There are no known workarounds.</p>
CSCsa64533	<p>The default modulation profiles for the MC5x20 line card are not optimized for Voice over IP (VoIP).</p> <p>If the intent is to run PacketCable VoIP with G711at 20 msec packetization without payload header suppression (PHS), the current default modulation profiles can be very inefficient.</p> <p>Workaround: Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Instead of profile 21, configure profile 22.</li> <li>2. Change the FEC CW size to 232.</li> <li>3. Change the FEC T bytes to 9.</li> <li>4. Repeat these steps for profiles 121 and 221.</li> </ol> <p>Note that other line cards, such as the MC28U, already have optimized modulation profiles.</p>

**Table 69**      **Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb21856	<p>Spectrum groups with discrete frequency entries are not supported on cable line cards containing Advanced Spectrum Management functionality.</p> <p>A warning message should be generated if such a spectrum-group is applied to an Advanced Spectrum Management capable upstream port.</p> <p>There are no known workarounds.</p>
CSCsb29361	<p>In some circumstances, a cable modem with a downstream minimum reserved rate is allowed to register on a Cisco uBR10000 series cable modem termination system (CMTS). However, committed information rate (CIR) resources for the modem are not available. Error messages similar to the following are displayed in the unit's log:</p> <pre data-bbox="574 684 1477 785">%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow 236, CM 0004.9e95.f2a9</pre> <p>The modem is not able to receive any downstream data.</p> <p>The issue occurs only when the total reserved downstream bandwidth approaches the total available downstream bandwidth.</p> <p>There are no known workarounds.</p>
CSCsb29718	<p>The customer premises equipment (CPE) does not complete the Dynamic Host Configuration Protocol (DHCP) when moved from behind one cable modem to another.</p> <p>The following event is logged:</p> <pre data-bbox="574 1115 1477 1236">...start... Jun 30 13:48:54.962: %UBR10000-3-SPOOFEDMAC: Investigating MAC=0011.2f32.c220 Cable6/1/0 sid 2900: Original MAC on sid 2899 Cable6/1/0 ...end...</pre> <p>Workaround: Enter the <b>clear cable modem</b> or <b>clear cable host</b> command.</p>

**Table 69**      **Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

DDTS ID Number	Description
CSCsb86099	<p>While performing a switchover, the following error message occurs. After multiple switchovers, the router unexpectedly crashes:</p> <pre>Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC2 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC3 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC4 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US2 Physical Port Link Down</pre> <p>This issue occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>• Performing a Route Processor Redundancy (RPR) switchover using the CLI.</li> <li>• Performing multiple switchovers</li> </ul> <p>There are no known workarounds.</p>
CSCsc12507	<p>When PacketCable event messaging is enabled, the cable modem termination system (CMTS) always uses the global routing table to find the route for the dynamically learned record keeping server (RKS) address. As a result, if the RKS IP address is part of a VPN routing/ forwarding (VRF) route table, CMTS fails to do the correct routing for the Remote Authentication Dial-In User Service (RADIUS) accounting messages.</p> <p>This issue occurs on a Cisco uBR10012 CMTS with a Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) based setup.</p> <p>Workaround: Perform a controlled route distribution between the VRF routing table and the global routing table so that the route for RKS server will be available on the global IPV4 routing table.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC02 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>

**Table 69 Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

DDTS ID Number	Description
CSCsc30294	<p>The following traceback occurs when testing line card failover while making a call from a Cisco uBR10000 series router.</p> <pre>Remote CMTS calls in progress CLI switchover working to protect. SLOT 5/0: Oct 25 17:25:20.871: %SCHED-3-STUCKMTR: Sleep with expired managed timer 62B2ABD4, time 0xE06B58 (00:00:00 ago). -Process= "Dynamic Services Timer Process", ipl= 4, pid= 40 -Traceback= 601306F0 60130B48 60283108</pre> <p>There are no known workarounds.</p>
CSCsc32241	<p>A single tunnel interface, in a configuration of more the 1000 tunnels, does not receive the multicast traffic that it should be receiving.</p> <p>This issue occurs only in configurations with more than 1000 tunnel interfaces.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsc35150	<p>If the <b>global hccp config</b> command is re-entered, the specified line card fails over.</p> <p>This issue occurs when you re-enter the <b>global hccp config</b> command and enter <b>Ctrl-Z</b> to exit. This action invokes an enter and exit at the same time and forces a line card failover.</p> <p>Workaround: To parse out the <b>config</b> command, delete the <b>config</b> command before you invoke <b>Ctrl-Z</b> or type <b>exit/end</b>. You can use <b>Ctrl-C</b> also. Either way, don't re-enter a <b>config</b> command that is already entered.</p>
CSCsc38875	<p>When a downstream cable interface on a Cisco uBR series router cable modem termination system (CMTS) experiences sustained congestion, and a significant portion of the downstream traffic is multicast traffic, Internet Group Management Protocol Version 2 (IGMPv2) Query messages might not be transmitted successfully in the downstream direction on that cable interface.</p> <p>The issue occurs when large volumes of multicast traffic, using groups that are not specified, use the cable interface <b>cable match address</b> command.</p> <p>Workaround: Ensure that all multicast traffic passing through the CMTS is classified with an appropriate <b>cable match address</b> command. This workaround may be effective only on Cisco uBR10000 series routers.</p>
CSCsc71939	<p>After a Performance Routing Engine (PRE) switchover followed by a line card (LC) switchover, if the Protect LC is reset or unexpectedly reloads, the standby PRE may crash due to a state inconsistency.</p> <p>There are no known workarounds.</p>
CSCsc81321	<p>The <b>vendor</b> option is missing from the <b>show cable modem</b> command. When specifying an interface, such as <b>show cable modem c4/0 vendor</b>, the <b>vendor</b> option does not work.</p> <p>Workaround: Use a command without a specific interface to get all interfaces, such as the <b>show cable modem vendor</b> command.</p>

**Table 69**      **Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsc91717	<p>There is a discrepancy in packet classification between the Fast Ethernet and Gigabit Ethernet interfaces.</p> <p>There are no known workarounds.</p>
CSCsd03740	<p>The <b>cable upstream 0 scheduling type ?</b> command is not synchronized during N+1 switchover.</p> <p>There are no known workarounds.</p>
CSCsd20606	<p>A parallel express forwarding (PXF) restart disables multicast traffic that matches the Multicast Quality of Service (MQoS) configuration.</p> <p>This issue occurs when an MQoS configuration is applied to cable interfaces, and PXF is restarted</p> <p>There are no known workarounds.</p>
CSCsd20683	<p>A command switchover with a virtual interface (VI) configuration is not switching the whole line card.</p> <p>By default, when VI is enabled on an interface, the Hot Standby Connection-to-Connection Protocol (HCCP) line card should switchover the whole line card instead of switching an individual domain.</p> <p>There are no known workarounds.</p>
CSCsd29450	<p>A Protect line card crashes after a sequence of route processor (RP) and LC switchovers.</p> <p>This issue occurs when performing a sequence of LC and Performance Routing Engine (PRE) switchovers.</p> <p>There are no known workarounds.</p>
CSCsd30267	<p>The Authentication, Authorization, and Accounting (AAA) per user process is holding memory, and the router is running out of memory.</p> <p>This issue occurs when PPP over Ethernet (PPPoE) dialing and dynamic access control lists (ACLs) are present.</p> <p>There is no known workaround.</p>
CSCsd31970	<p>On a Cisco uBR10000 series router cable modem termination system (CMTS) with redundant Performance Routing Engine (PRE) modules, new interface mode configuration commands entered on the active PRE may not be properly synchronized to the standby PRE if the <b>do show running-configuration</b> command is entered in interface configuration mode.</p> <p>This issue can lead to a configuration mismatch between the two PRE modules and can cause difficulty on PRE switchover.</p> <p>Workaround: Refrain from issuing the <b>do show running-configuration</b> command in interface configuration mode, or completely exit interface configuration mode after issuing the command.</p>

Table 69 Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)

DDTS ID Number	Description
CSCsd33394	<p>On a Cisco uBR10000 series routers cable modem termination system (CMTS), upstream subscriber traffic management filters do not filter packets with a multicast destination IP address.</p> <p>Workaround: Configure and apply an IP access-list to the cable or bundle interface that applies to traffic for all the modems and customer premises equipment (CPE) on the interface.</p>
CSCsd36652	<p>When configuring line card redundancy by using the <b>global HA</b> commands, duplicate RF-switch slot numbers were configured. This configuration is not allowed.</p> <p>There are no known workarounds.</p>
CSCsd43741	<p>VID data in the entPhysicalHardwareRev MIB displays the wrong value if the data field in EEPROM is missing.</p> <p>This issue affects the Entity MIB in all Cisco uBR10000 software releases, if the VID data field is not programmed.</p> <p>There are no known workarounds.</p>
CSCsd44373	<p>Certain upstream (US) parameters are not copied from a Working cable line card (CLC) to the Protect CLC during a failover under the following conditions: -upstream docsis mode, -upstream modulation profile, -upstream data-backoff.</p> <p>Because the original settings on the Protect CLC remain, it is possible after a failover to have a Data-over-Cable Service Interface Specification (DOCSIS) mode and modulation profile inconsistent with that of the Working CLC prior to the failover. This inconsistency can create problems. For example, if a Time Division Multiple Access (TDMA)-only Working CLC fails over to a Protect CLC configured with Asynchronous Time Division Multiple Access (ATDMA), the cable modems will switch to ATDMA mode. When the Protect fails back to the TDMA-only Working CLC, the cable modems will continue to use ATDMA and lose IP connectivity.</p> <p>There are no known workarounds.</p>
CSCsd47667	<p>The cable meter feature is causing redundancy to fail between PRE2s due to Inter-Process Communication (IPC) timeouts.</p> <p>This issue occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC2 or 12.3(17a)BC.</p> <p>Workaround: Reload the standby PRE2.</p>
CSCsd65022	<p>The downstream (DS) bandwidth scheduler doesn't work correctly after a PacketCable Multimedia (PCMM) call switchover.</p> <p>There are no known workarounds except to reload the cable modem termination system (CMTS).</p>
CSCsd67236	<p>A policy-based routing (PBR) map with a set clause does not act on matching packets.</p> <p>This issue occurs on PRE1s on Cisco uBR10000 series routers only.</p> <p>There are no known workarounds.</p>

**Table 69** Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)

DDTS ID Number	Description
CSCsd73128	<p>A voice call is not fully recovered until 6 seconds after a CLI LC switchover.</p> <p>Workaround: Enter the <b>cable sync-interval 2</b> command on all Working and Protect interfaces before attempting a switchover.</p>
CSCsd77991	<p>A line card on the Cisco uBR10000 series router unexpectedly crashes.</p> <p>This issue occurs when the <b>clear cable modem</b> command is executed for multicast address.</p> <p>Workaround: Do not use the <b>clear cable modem</b> command for multicast addresses.</p>
CSCsd78370	<p>The privacy bit value of the Multicast entries present on the cable modem termination system (CMTS) host database change after a Route Processor Redundancy (RPR) switchover.</p> <p>This issue occurs when adding multicast entries into the CMTS host database but before the RPR Switchover.</p> <p>There are no known workarounds.</p>
CSCsd95113	<p>A cable modem, when enforced with a quality of service (QoS) profile created using the cdxCmtsCmQosProfile MIB, accepts the profile and <b>show cable modem reg</b> shows the modem with the enforced profile. However, the same cable modem, after reset, does not come online with the enforced profile. Instead, it comes online with the default profile. In contrast, the same modem (when enforced with the QoS profile created using the CLI) comes online after reset with the enforced profile, not the default profile.</p> <p>This behavior is the same irrespective of platforms and whether the QoS profile is created using the CLI or Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCse00902	<p>Various <b>show</b> commands use improper case and spelling.</p> <p>There are no known workarounds.</p>
CSCse02543	<p>When some modems are in the reject state and a <b>clear cable modem reject delete</b> command is issued, a CM_INCONSISTENCY message is generated.</p> <p>Workaround: Do not use the <b>clear cable modem reject delete</b> command.</p>
CSCse08883	<p>After two Performance Routing Engine (PRE) switchovers, a non-functioning High Availability (HA) LC becomes active on the PROTECTA MC520H line card.</p> <p>There are no known workarounds.</p>
CSCse22482	<p>After a Performance Routing Engine (PRE) failover, downstream voice traffic moves from dynamic flow to primary flow.</p> <p>There are no known workarounds.</p>

Table 69 Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)

DDTS ID Number	Description
CSCse24904	<p>When a lockout of the Working card is followed by online insertion and removal (OIR), the following two problems occur: 1) OIR switches from the Working card to the Protect card, dropping all the cable modems. 2) After the Working card is back from the OIR, traffic stays on the Protect card with the cable modems down, and the Working card has lockout active. Clearing lockout fails, and because the Working card is standby, reverting to the Working card would also fail.</p> <p>There are no known workarounds.</p>
CSCse25969	<p>The standby Performance Routing Engine (PRE) crashes at cmts_adm_ctrl_bw_init_mschedp_type.</p> <p>The crash occurs only while booting the standby PRE.</p> <p>There are no known workarounds.</p>
CSCse27391	<p>The Hot Standby Connection-to-Connection Protocol (HCCP) stops working properly when a switchover is required from the Working card to the Protect card. No errors are shown. Switching back to the Working card gets the cable modems back online.</p> <p>Workaround: Reload the box; a reload/reseat of the line cards does not work.</p>
CSCse32310	<p>An MC520 crash occurs.</p> <p>There are no known workarounds.</p>
CSCse32901	<p>Overlapping RF switch slots numbers are configured in a global High Availability (HA) 4+1 setup.</p> <p>There are no known workarounds.</p>
CSCse43344	<p>The user can experience bad voice quality, if Low Latency Queueing (LLQ) is configured without enabling Admission Control (AC).</p> <p>This issue occurs when the user configures upstream scheduler mode with LLQ.</p> <p>Workaround: Enable AC after you have configured upstream (US) LLQ.</p>
CSCse45342	<p>Configuring cable default-tos-qos10 tos-overwrite and resetting the modem does not create a new qos-profile. The modem comes online with the existing profile.</p> <p>The problem occurs on modems provisioned in Data-over-Cable Service Interface Specification (DOCSIS) 1.0 mode when the default tos-mask and tos-value are configured.</p> <p>There are no known workarounds.</p>
CSCse48454	<p>Entering a <b>shut/no shut</b> command on an interface triggers infinite switchovers.</p> <p>There are no known workarounds.</p>
CSCse50735	<p>After a cable line card failover, the dynamic Service Flow (SF)-to-Multiprotocol Label Switching (MPLS) virtual private network (VPN) mapping feature no longer works.</p> <p>There are no known workarounds.</p>

**Table 69**      **Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCse54378	<p>On a Cisco uBR10000 series router running Cisco IOS image ubr10k-k9p6u2-mz.2006-06-02.123_17_BC, tracebacks are found at sch_rp_download_debug_info when you attempt to configure an already assigned address.</p> <p>There are no known workarounds.</p>
CSCse55592	<p>Two typos exist in the microcode under the Cisco uBR10000 PRE2 platform that can potentially result in some feature errors (including Input/Output ACL, MLP Rx, MLP Tx, MAC Rewrite, and WRED Calc.)</p> <p>There are no known workarounds.</p>
CSCse56676	<p>The cdrqCmtsCmRQDoneNotification trap, which indicates that the cable remote-query function has finished a polling cycle for modems on the cable modem termination system (CMTS), is sent to Simple Network Management Protocol (SNMP) management stations, even when cable specific traps are not configured to be sent to those stations.</p> <p>This condition occurs on a Cisco uBR series CMTS, and can occur on any trap sent, even when the trap is not associated with the SNMP host.</p> <p>There are no known workarounds.</p>
CSCse57637	<p>The Low Latency Queueing (LLQ) upstream scheduler option does not distinguish between Non Real Time Polling Service (nrtPS) and Real Time Polling Service (rtPS) flows correctly.</p> <p>There are no known workarounds.</p>
CSCse64138	<p>When load-balancing is used, some modems might go into init(rc) after an upstream channel change (UCC).</p> <p>There are no known workarounds.</p>
CSCse67808	<p>The cdpCacheTable contains entries with index 4294967295 that are only available using the Simple Network Management Protocol (SNMP) <b>get-next</b> command. When the <b>get-one</b> command is used to retrieve the same value, the NO_SUCH_INSTANCE_EXCEPTION is returned.</p> <p>This issue appears to be related to the management ethernet port on the secondary Performance Routing Engine (PRE) in a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCse67868	<p>The Simple Network Management Protocol (SNMP) cpmCPUTotalPhysicalIndex object returns valid entPhysicalIndex values for cable line cards (CLCs) when these values are retrieved using the <b>getnext</b> command, but when the <b>getone</b> command is used, the physical index values for the CLCs are returned as 0.</p> <p>This issue occurs on Cisco uBR10000 series routers with CLCs and SNMP configured</p> <p>There are no known workarounds.</p>

Table 69 Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)

DDTS ID Number	Description
CSCse69641	<p>When the <b>show cable modem s t</b> command is issued soon after a <b>clear cable modem all delete</b> command, the console and vty get stuck.</p> <p>The issue occurs in large-scale environments with more than 5000 modems.</p> <p>Workaround: Do not use the <b>clear cable modem all delete</b> command; delete specific modems instead.</p>
CSCse71725	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>cable monitor</b> command does not successfully monitor upstream bandwidth request messages.</p> <p>There are no known workarounds.</p>
CSCse78143	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>show cr10k-rp cable x/y/z sid</b> command does not allow the service identifier (SID) value to be set to values greater than 8176. As a result, queues associated with downstream multicast quality of service (QoS) SIDs cannot be examined.</p> <p>There are no known workarounds.</p>
CSCse80641	<p>The Transparent LAN Service (TLS) feature does not support stacked dot1q tags.</p> <p>This condition occurs when the TLS feature is configured, and the cable modem termination system (CMTS) receives a 1522 bytes packet (including the frame check sequence(FCS)) in the upstream direction that contains an 802.1q tag.</p> <p>There are no known workarounds.</p>
CSCse81859	<p>On a Cisco uBR10012 router running on Cisco IOS Release 12.3(13a)BC2, the Cisco uBR10-MC5X20U line card crashed with the following error:</p> <p>Cause 80000010 (Code 0x4): Address Error (load or instruction fetch) exception Crash info file was written and the LC was reloaded</p> <p>There are no known workarounds.</p>
CSCse82337	<p>The on-board Fast Ethernet board (interface fastethernet 0/0/0) does not recognize that the line protocol is down.</p> <p>This issue occurs after reloading the PRE2.</p> <p>Workaround: Enter <b>shut /no shut</b> on the interface, or reload the PRE2 again.</p>
CSCse85188	<p>On a Cisco cable modem termination system (CMTS), the quality of service (QoS) profile value for the maximum downstream burst is not displayed correctly and may not be set correctly after a reload.</p> <p>This issue occurs when the maximum downstream burst for a QoS profile is configured using the <b>cable qos profile n max-ds-burst value</b> command with a <i>value</i> greater than 2147483647. The value will be displayed as a negative number in the <b>show run</b> command output. If the configuration is written to memory, the maximum downstream burst is also saved as a negative number. As a result, this value is not processed correctly when the configuration is processed after a reload.</p> <p>There are no known workarounds. (Note that the <b>cable qos profile</b> command has been deprecated for Data-over-Cable Service Interface Specification (DOCSIS) 1.1 use because DOCSIS 1.1 replaces the QoS profile with a service flow, which is configured using the <b>cable service class</b> command.</p>

**Table 69**      **Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCse86436	<p>Massive Embedded Media Terminal Adapter (eMTA) flapping occurs after long hours of more than 1000 PacketCable Multimedia (PCMM) calls. All flapping eMTAs re-register back.</p> <p>There are no known workarounds.</p>
CSCse86458	<p>Many Arris Embedded Media Terminal Adapters (eMTAs) on an Asynchronous Time Division Multiple Access (ATDMA) channel go offline after an MC520u CLI switchover with PacketCable calls.</p> <p>There are no known workarounds.</p>
CSCse88914	<p>The total of exclusive bandwidth allocated to various service class names of a particular scheduling type exceeds the exclusive allocation configured for that scheduling type.</p> <p>There are no known workarounds.</p>
CSCse97227	<p>The cable modem termination system (CMTS) crashes while un-configuring global Hot Standby Connection-to-Connection Protocol (HCCP) configurations.</p> <p>This issue occurs only when the global HCCP configuration includes slot numbers that are not present in the CMTS.</p> <p>There are no known workarounds.</p>
CSCse98224	<p>About 10 minutes after loading Cisco IOS Release 12.3(17a)BC2 on a Cisco uBR10000 series router with about 5000 cable modems and digital set-top boxes (STBs) connected, the operator was unable to ping to directly connected Backbone Switches' interfaces on the Cisco uBR10000 router, and the Open Shortest Path First (OSPF) neighbor with the Backbone Switches (OSRs) was in the DOWN state. The Gigabit Ethernet interfaces' state was UP, and the only log message to appear was that the OSPF neighbor's state was down.</p> <p>There are no known workarounds.</p>
CSCse99462	<p>Spurious Accesses traceback occurs. The static Hot Standby Connection-to-Connection Protocol (HCCP) sync keeps sync, but is not able to resolve, because the STATICSYNCDONE is not received,</p> <p>This issue occurs in an N+1 global configuration, after the line card switchover but before the sync is completed, and when flapping one port of Protected interface (in the HCCP active state)</p> <p>Workaround: Do not flap the HCCP active interface before the sync completes.</p>
CSCsf00801	<p>Internet Control Message Protocol (ICMP) packets are captured on the cable monitoring interface where they shouldn't be replicated when the cable monitor interface FastEthernet0/0/0 access-list [2] [packet-type ethernet] is configured on the cable line card.</p> <p>This issue can occur both upstream and downstream, and regardless of access list type: numbered, named, standard or extended.</p> <p>There are no known workarounds.</p>
CSCsf02972	<p>When moving upstreams with more than 500 cable modems to an upstream port on the Cisco uBR10k series router, some modems do not come online.</p> <p>Workaround: Change the upstream frequency to get them to come online.</p>

Table 69 Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)

DDTS ID Number	Description
CSCsf02982	<p>When an attempt is made to modify the in-use Peer-to-Peer (P2P) policy, an error occurs.</p> <p>There are no known workarounds.</p>
CSCsf04338	<p>The Cisco uBR series cable modem termination system (CMTS) with cable or bundle subinterfaces configured does not prevent customer premises equipment (CPE) from receiving a Dynamic Host Configuration Protocol (DHCP) offer with an IP address belonging to the wrong subinterface. Only DHCP offers that contain an offered IP address within the same subinterface as the cable modem belonging to the customer premises equipment (CPE) should be forwarded by the CMTS.</p> <p>The issue occurs when the CMTS is configured to use cable or bundle subinterfaces and the DHCP server is wrongly configured.</p> <p>Workaround: Ensure that the DHCP server is configured to assign CPE devices IP addresses from only the appropriate IP subnets.</p>
CSCsf07848	<p>On a Cisco uBR series cable modem termination system (CMTS), the Embedded Media Terminal Adapter (eMTA) component of a PacketCable enabled device cannot get IP connectivity if another customer premises equipment (CPE) device in the system has previously used the MAC address of the eMTA.</p> <p>Workaround: Issue the clear cable host affected-mac-address command to release control of the affected mac address and to allow the eMTA to take ownership of that MAC-address.</p>
CSCsf10689	<p>For some cable upstream interfaces, no entry exist in the DOCS-IF-MIB and the CISCO-CABLE-SPECTRUM-MIB.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.2(15)BC2e and Cisco IOS Release 12.2(15)BC5.</p> <p>There are no known workarounds.</p>
CSCsf12149	<p>While deleting the second stream intercept, the Simple Network Management Protocol (SNMP) returns with a COMMIT_FAILED_ERROR. The <b>getmany</b> command shows that the stream is actually deleted.</p> <p>This issue occurs when each stream has a different protocol value, each stream is associated with different MD, and an attempt is trying to delete the second stream.</p> <p>Workaround: Ignore the error message; the stream is actually deleted.</p>
CSCsf18311	<p>An RF line card failover occurs as a result of powering down the Working line card.</p> <p>There are no known workarounds.</p>
CSCsf19110	<p>In a large-scale setup with more than 5000 modems, if you copy a baseline privacy interface (BPI)- enabled configuration file and enter the <b>clear cable modem all del</b> command, after at least 4000 modems are up, tracebacks and memory alloc failure messages are found on the MC520u cards.</p> <p>There are no known workarounds.</p>
CSCsf22037	<p>The cable sflog maximum entry value needs to be changed to 1-59999</p> <p>There are no known workarounds.</p>

**Table 69**      **Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

DDTS ID Number	Description
CSCsf27296	<p>If two line cards failover to the Protect card at the same time, the Performance Routing Engine (PRE) can crash/ failover shortly afterwards. While a majority of the modems recover, some get stuck from init(rc) to init(o).</p> <p>This issue occurs on a Cisco uBR10000 series router with PRE2, MC520s, and MC520u cards running Cisco IOS Release 12.3(9a)BC8.</p> <p>Workaround: Try resetting the PRE, or resetting Parallel Express Forwarding (PXF) through the CLI.</p>
CSCsf29154	<p>The communication between the line cards and the routing processor fails. The output of <b>show diag</b> command is empty.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC1.</p> <p>Workaround: Reload the router.</p>
CSCsf30877	<p>The wrong classification is applied to the IP Protocol field.</p> <p>There are no known workarounds.</p>
CSCsf31242	<p>The <b>show cable modem cpe_ip</b> command should display information about the cable modem with which a customer premises equipment (CPE) device is associated, but does not.</p> <p>This issue is seen on one cable modem termination system (CMTS), multiple line cards, and multiple upstream/downstreams. This issue recurs intermittently, a few times a month, with no known cause.</p> <p>Workaround: Enter the <b>clear cable modem delete</b> command to work around the issue.</p>
CSCsf33128	<p>All the wideband cable modems in the cable modem termination system (CMTS) reset when a configuration file is uploaded from disk to become the running configuration. All the modems return online after the reset and function properly.</p> <p>This issue occurs only when spectrum management has been configured in the configuration file.</p> <p>Workaround: Remove the spectrum management configuration from the configuration file.</p>
CSCsf96635	<p>The following error message, followed by a traceback occurs on the router after a period of normal operation:</p> <pre>%GENERAL-3-EREVENT: HWCEF: Loadinfo fastadj lock with NULL fasttag_rew</pre> <p>There are no known workarounds.</p>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>

**Table 69** Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)

DDTS ID Number	Description
CSCsf99847	A Cisco uBR10000 series router running ubr10k-k8p6-mz.123-9a.BC9 crashes with an unexpected exception, CPU signal 23: "%SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 63AD71B0, data B0D0B0D"  There are no known workarounds.
CSCsg03719	Tracebacks and spurious memory accesses occur after a Performance Routing Engine (PRE) switchover.  This issue occurs in a large-scale testbed with more than 5000 modems.  There are no known workarounds.
CSCsg16433	The mac-address in the metering file is wrong. Instead of the management interface address it shows the mac-address of the first interface in the <b>show ip interface brief</b> list.  There are no known workarounds.
CSCsg16781	A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).  Workaround: Try to configure a stream from subnet which is present on the CMTS.
CSCsg17050	The DOCSIS Set-Top Gateway (DSG) interface configuration is not retained when a 5X20S card is replaced with a 5x20U card, and vice versa.  Workaround: Remove the dsg tg configuration from the global configuration, configure it again, and apply the configuration to the interface.
CSCsg17576	The Cisco uBR10012 MC520u upstream PHY TI4522 receiver does not work correctly with the Data-over-Cable Service Interface Specification (DOCSIS) 2.0 Reed Solomon dynamic interleaver.  When a customer creates a modulation profile that includes Asynchronous Time Division Multiple Access (ATDMA) interval usage code (IUC) values, such as A-LONG, with dynamic interleaver enabled it can cause the upstream port to lose data over time for the ATDMA modems and can also cause the signal-to-noise ratio (SNR) reported for those upstreams to report very poor SNR values minutes after traffic passes on those ports.  Workaround: Ensure your modulation profile does not have dynamic interleaver enabled for any A-DMA IUC elements, such as A-LONG or A-UGS.
CSCsg21610	If the minimum information rate (MIR) of a service flow is specified as zero (or unspecified) and best effort service flow policing is enabled, the best effort service flow rate is limited to 64Kbps.  Workaround: Specify an MIR value for best effort service flows.
CSCsg25638	An MC520u line card in a Cisco uBR10000 cable modem termination system (CMTS) spontaneously reloads.  This issue occurs on a CMTS running Cisco IOS Release 12.3(9a)BC7.  There are no known workarounds.

**Table 69**      **Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)**

DDTS ID Number	Description
CSCsg27690	<p>A traceback is generated if the card configuration that is the upper slot of an Spatial Reuse Protocol (SRP) card pair is removed (no card) from the running configuration while the SRP interface has an output service policy applied.</p> <p>Workaround: If the service policy is removed from the SRP interface prior to the upper slot card being un-configured, the traceback is not generated.</p>
CSCsg30121	<p>If the <b>debug cable mac-address</b> command is enabled and the cable monitor is configured, <b>cable monitor debug</b> outputs flood the console.</p> <p>This issue occurs even if the debug and cable monitor commands are for different devices. The amount of these packets generated can be very large and can be a great annoyance on the console.</p> <p>There are no known workarounds.</p>
CSCsg32252	<p>A Cisco uBR10-MC5X20U card reports an impossibly low upstream (US) signal-to-noise ratio (SNR) for Quadrature Amplitude Modulation 16 (QAM16) with some working cable modems. However, the affected subscribers do not report any problems.</p> <p>Reportedly, the problem was not seen before the hardware upgrade from MC28/UBR7200 to MC5x20/UBR10K.</p> <p>Workaround: Rely on the error counters, rather than on the SNR readings.</p>
CSCsg34038	<p>The ifDescr Snmp query returns a negative value when the subinterface bundle is configured with the maximum subinterface number allowed.</p> <p>Workaround: Do not configure the maximum subinterface number when configuring the subinterface bundle.</p>
CSCsg38426	<p>In a system with 40 virtual interface bundles, assigning one of those virtual interface bundles to all mac domains in a fully loaded chassis, generates the following message on the console after deleting the assigned virtual interface bundle:</p> <pre data-bbox="613 1287 1528 1339">*MCASTECHO: All DS Group Index has been used up. Interface: Cable6/1/4 VCCI:: 33.</pre> <p>There are no known workarounds.</p>
CSCsg39288	<p>Backup TCC card may experience a reload (IPCOIR-3-TIMEOUT on TCC card).</p> <p>The issue has been experienced on 12.3(9a)BC9, 12.3(13a)BC2 and 12.3(13a)BC6. There are compare errors in the <b>show controllers clock-reference</b> that do increment. However the clocks are not actually drifting apart, even though the errors are incrementing. Because clocks are not actually drifting, redundancy is not affected, except during the brief period when the backup TCC+ card reloads after a IPCOIR timeout.</p> <p>There are no known workarounds.</p>
CSCsg39990	<p>Cable filter groups do not filter local traffic on the Cisco uBR10000 platform.</p> <p>There are no known workarounds.</p>

Table 69 Open Caveats for Cisco IOS Release 12.3(17b)BC4 (continued)

DDTS ID Number	Description
CSCsg44938	<p>A swap between the MC520h card and MC520u card forces the first JIB's downstreams into the shutdown state. For instance, if you downgrade from the MC520H card to the MC520u card, the MC520u card will shutdown Cx/y/0 and Cx/y/2 to build its configuration.</p> <p>This issue occurs on a Cisco uBR10000 series router running an interface-level Hot Standby Connection-to-Connection Protocol (HCCP) configuration on Cisco IOS Release 12.3(17a)BC2, with the <b>cr10k card slot/subslot oir-compatibility</b> command enabled.</p> <p>There are no known workarounds.</p>
CSCsg45576	<p>The router can unexpectedly restart during line card online insertion and removal (OIR) if the execution of the <b>show pxf cpu queue</b> command is preempted by the <b>More</b> prompt, and the command output is allowed to continue after the line card has fully initialized.</p> <p>Workaround: Allow the command output to complete before performing an OIR of the associated line card.</p>
CSCsg45692	<p>The Cisco uBR10K 5X20 line card crashes at cr10k_clc_pre_poll.</p> <p>This issue occurs on Cisco IOS Release 12.3(13a)BC6 or Cisco IOS Release 12.3(9a)BC7.</p> <p>There are no known workarounds.</p>
CSCsg46284	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC6 may not generate a crashinfo file for the uBR10K-MC5x20U-D line card.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(17b)BC4

Table 70 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC4.

**Table 70** Resolved Caveats for Cisco IOS Release 12.3(17b)BC3

DDTS ID Number	Description
CSCsf31762	<p>Some packets are not dequeued from a cable interface, causing the input queue size to increase beyond the maximum configured queue size. As a result, traffic drops and modems go offline.</p> <p>This issue occurs on the 5cable-mc520s-d card on the Cisco uBR10000 platform, and appears to be caused by a particular (possibly corrupted) packet.</p> <p>Workaround: To temporarily fix the problem, increase the queue size using the <b>hold-queue</b> command.</p>
CSCsg31641	<p>After a switchover between Performance Routing Engines (PREs), the Transparent LAN Service (TLS) stops passing traffic to the Gigabit Ethernet interface until another switchover occurs. (The TLS configuration remains identical on both PREs before and after the switchover.)</p> <p>This issue is specific to the Half-Height Gigabit Ethernet (HHGE) line card and occurs as a result of a redundancy switchover and a Gigabit Ethernet interface reset.</p> <p>Workaround: Remove the TLS configuration on the active PRE and then re-add it again.</p>
CSCsg34910	<p>Support was added to allow load balancing to even out upstream (US) load balancing (LB) group members.</p>
CSCsg45624	<p>Unexpected downstream packet loss occurs within the 5x20H Cable line card during periods of congestion.</p> <p>Workaround: There are no known workarounds with the exception of trying to prevent the congestion from occurring.</p>

## Open Caveats for Release 12.3(17b)BC3

Table 71 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC3.

**Table 71** Open Caveats for Cisco IOS Release 12.3(17b)BC3

DDTS ID Number	Description
CSCef66578	<p>The output of the <b>show cable modem connectivity</b> command displays an extremely large value.</p> <p>This issue occurs in Cisco IOS Releases 12.2(15)BC2b and 12.2(15)BC2c.</p> <p>There are no known workarounds.</p>
CSCeg30757	<p>A standby Performance Routing Engine (PRE) reloads unexpectedly. There is no impact on the primary PRE, and the router continues to function as normal.</p> <p>This issue occurs only when a Hot Standby Connection-to-Connection Protocol (HCCP) switchover is enabled through the command line interface on the router.</p> <p>Workaround: There are no known workarounds, other than to avoid enabling the HCCP switchover.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>
CSCej52423	<p>The wrong number of bytes are suppressed and packet drops occur on the dial shelf controller (DSC) when adding payload header suppression (PHS) and line card (LC) switchover.</p> <p>This issue occurs when performing a switchover while using LC redundancy and Multiple PHS for a secondary service flow (SF).</p> <p>Workaround: Do not use PHS with multiple rules for an SF if you are using N+1.</p>
CSCek21720	<p>Traceback occurs with packet intercept during a line card (LC) switchover in PRE2.</p> <p>This issue occurs when the LC switchover is performed while PacketCable (PC) calls and class features are in progress.</p> <p>There are no known workarounds</p>

Table 71 Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)

DDTS ID Number	Description
CSCek23320	<p>Simple Network Management Protocol (SNMP)-related traceback occurs when the image is loaded with the attached cable modem termination system (CMTS) configuration:</p> <pre>*Dec 21 16:11:28.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/1, changed state to up Dec 21 16:12:08.141: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61156234 reading 0x0 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 61156234 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 6115623C 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:14:11.138: %AAAA-3-DROPACCTSNDFAIL: Accounting record dropped, send to server failed: system-start</pre> <p>There are no known workarounds.</p>
CSCek24075	<p>Zero nodes are reported in the <b>show srp topology</b> command.</p> <p>There are no known workarounds.</p>
CSCek27678	<p>The <b>show access-list</b> command displays the access control lists (ACLs) for deleted packet filter groups. The corresponding internal ACLs are not removed, even after the packet filter group is deleted.</p> <p>The <b>show cable filter</b> command lists the reserved ACL group 255 index 1 with drop action, even if all the cable filter configurations have been removed from the cable modem termination system (CMTS).</p> <p>There are no known workarounds.</p>
CSCek31526	<p>The Inter-Process Communication (IPC) between cable line cards (CLCs) occasionally fails.</p> <p>Workaround: Reload the image to fix this issue.</p>
CSCek34311	<p>The Performance Routing Engine (PRE) unexpectedly reloads if the <b>cable upstream n frequency up-freq-hz</b> command is repeated more than 500 times.</p> <p>There are no known workarounds.</p>
CSCek35970	<p>The IP ToS/DSCP byte is not overwritten for PacketCable CALEA replicated packets with the value received by GATE-SET COPS messages.</p> <p>There are no known workarounds.</p>
CSCek37518	<p>Client information is not displayed in the <b>show cable dsg tunnel ?</b> command when the tunnel group is not associated with a downstream interface.</p> <p>There are no known workarounds.</p>
CSCek38598	<p>No corresponding parallel express forwarding (PXF) queue is created for the new dynamic service flow when testing the dynamic service messaging (DSX) with the <b>test cable DSA</b> command.</p> <p>The real Media Terminal Adapters (MTAs) are able to make call with DSX without any problem.</p> <p>There are no known workarounds.</p>
CSCek39428	<p>DC Directory (DCD) messages do not get captured if the <i>mac-address</i> parameter is specified in the <b>cable monitor</b> command.</p> <p>There are no known workarounds.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCek42764	<p>After an LC switchover, the working standby interface configuration is displayed in the <b>show dsgr tunnel</b> output.</p> <p>Workaround: Skip the standby interface when scanning cable interfaces to display the DOCSIS Set-Top Gateway (DSG) tunnel information.</p>
CSCek48531	<p>A miscreant user alters the MAC address of their cable modem to match the MAC address of another cable modem on the same cable modem termination system (CMTS) chassis in an attempt to steal service by impersonating the legitimate user. Instead, the legitimate user is taken offline constantly, and neither modem stays online for more than 10-30 seconds. CMTS logs show a <code>CM_MOVED</code> message each time the modem moves from port to port. CMTS logs may show a Spoof or bad QoS registration message if the modem is on the same port, or may not show any logs.</p> <p>This condition can occur when the modem is one of several cable modem models susceptible to this modification. These models represent about 1/3 of all cable modems deployed worldwide.</p> <p>Workaround: There are no known workarounds other than to replace the legitimate user's cable modem with a new one. The legitimate user is always taken offline.</p>
CSCek59655	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC6 reloads in production environment</p> <p>There are no known workarounds.</p>
CSCin98031	<p>N+1 synchronization does not occur when switching over from the Working card to the Protect card.</p> <p>There are no known workarounds.</p>
CSCsa53610	<p>The router fails to come up in Route Processor Redundancy (RPR) mode.</p> <p>This condition is caused by the fix for CSCef64718, which moved around the time point of posting <code>PEER_COMM</code> loss at switchover.</p> <p>There are no known workarounds.</p>
CSCsa64533	<p>The default modulation profiles for the MC5x20 line card are not optimized for Voice over IP (VoIP).</p> <p>If the intent is to run PacketCable VoIP with G711 at 20 msec packetization without payload header suppression (PHS), the current default modulation profiles can be very inefficient.</p> <p>Workaround: 1) Instead of profile 21, configure profile 22. 2) Change the FEC CW size to 232. 3) Change the FEC T bytes to 9. 4) Repeat these steps for profiles 121 and 221. Note that other line cards, such as the MC28U, already have optimized modulation profiles.</p>
CSCsb21856	<p>Spectrum-groups with discrete frequency entries are not supported on cable line cards containing Advanced Spectrum Management functionality.</p> <p>A warning message should be generated if such a spectrum-group is applied to an Advanced Spectrum Management capable upstream port.</p> <p>There are no known workarounds.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCsb29361	<p>In some circumstances, a cable modem with a downstream minimum reserved rate is allowed to register on a Cisco uBR10000 series cable modem termination system (CMTS). However, committed information rate (CIR) resources for the modem are not available. Error messages similar to the following are displayed in the unit's log:</p> <pre data-bbox="613 489 1523 590">%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow 236, CM 0004.9e95.f2a9</pre> <p>The modem is not able to receive any downstream data.</p> <p>The issue occurs only when the total reserved downstream bandwidth approaches the total available downstream bandwidth.</p> <p>There are no known workarounds.</p>
CSCsb29718	<p>The customer premises equipment (CPE) does not complete the Dynamic Host Configuration Protocol (DHCP) when moved from behind one cable modem to another.</p> <p>The following event is logged:</p> <pre data-bbox="613 915 1523 1041">...start... Jun 30 13:48:54.962: %UBR10000-3-SPOOFEDMAC: Investigating MAC=0011.2f32.c220 Cable6/1/0 sid 2900: Original MAC on sid 2899 Cable6/1/0 ...end...</pre> <p>Workaround: Enter the <b>clear cable modem</b> or <b>clear cable host</b> command.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCsb86099	<p>While performing a switchover, the following error message occurs. After multiple switchovers, the router unexpectedly crashes:</p> <pre>Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC2 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC3 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC4 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US2 Physical Port Link Down</pre> <p>This issue occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>• Performing a Route Processor Redundancy (RPR) switchover using the CLI.</li> <li>• Performing multiple switchovers</li> </ul> <p>There are no known workarounds.</p>
CSCsc12507	<p>When PacketCable event messaging is enabled, the cable modem termination system (CMTS) always uses the global routing table to find the route for the dynamically learned record keeping server (RKS) address. As a result, if the RKS IP address is part of a VPN routing/ forwarding (VRF) route table, CMTS fails to do the correct routing for the Remote Authentication Dial-In User Service (RADIUS) accounting messages.</p> <p>This issue occurs on a Cisco uBR10012 CMTS with a Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) based setup.</p> <p>Workaround: Perform a controlled route distribution between the VRF routing table and the global routing table so that the route for RKS server will be available on the global IPV4 routing table.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC02 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>

Table 71 Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)

DDTS ID Number	Description
CSCsc30294	<p>The following traceback occurs when testing line card failover while making a call from a Cisco uBR10000 series router.</p> <pre>Remote CMTS calls in progress CLI switchover working to protect. SLOT 5/0: Oct 25 17:25:20.871: %SCHED-3-STUCKMTMR: Sleep with expired managed timer 62B2ABD4, time 0xE06B58 (00:00:00 ago). -Process= "Dynamic Services Timer Process", ipl= 4, pid= 40 -Traceback= 601306F0 60130B48 60283108</pre> <p>There are no known workarounds.</p>
CSCsc32241	<p>A single tunnel interface, in a configuration of more the 1000 tunnels, does not receive the multicast traffic that it should be receiving.</p> <p>This issue occurs only in configurations with more than 1000 tunnel interfaces.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the output from the <b>show interface</b> command are 10% of the actual packet and bit rates.</p> <p>This issue occurs only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsc35150	<p>If the <b>global hccp config</b> command is re-entered, the specified line card fails over.</p> <p>This issue occurs when you re-enter the <b>global hccp config</b> command and enter <b>Ctrl-Z</b> to exit. This action invokes an enter and exit at the same time and forces a line card failover.</p> <p>Workaround: To parse out the <b>config</b> command, delete the <b>config</b> command before you invoke <b>Ctrl-Z</b> or type <b>exit/end</b>. You can use <b>Ctrl-C</b> also. Either way, don't re-enter a <b>config</b> command that is already entered.</p>
CSCsc38875	<p>When a downstream cable interface on a Cisco uBR series router cable modem termination system (CMTS) experiences sustained congestion, and a significant portion of the downstream traffic is multicast traffic, Internet Group Management Protocol Version 2 (IGMPv2) Query messages might not be transmitted successfully in the downstream direction on that cable interface.</p> <p>The issue occurs when large volumes of multicast traffic, using groups that are not specified, use the cable interface <b>cable match address</b> command.</p> <p>Workaround: Ensure that all multicast traffic passing through the CMTS is classified with an appropriate <b>cable match address</b> command. This workaround may be effective only on Cisco uBR10000 series routers.</p>
CSCsc71939	<p>After a Performance Routing Engine (PRE) switchover followed by a line card (LC) switchover, if the Protect LC is reset or unexpectedly reloads, the standby PRE may crash due to a state inconsistency.</p> <p>There are no known workarounds.</p>
CSCsc81321	<p>The <b>vendor</b> option is missing from the <b>show cable modem</b> command. When specifying an interface, such as <b>show cable modem c4/0 vendor</b>, the <b>vendor</b> option does not work.</p> <p>Workaround: Use a command without a specific interface to get all interfaces, such as the <b>show cable modem vendor</b> command.</p>

Table 71 Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)

DDTS ID Number	Description
CSCsc91717	<p>There is a discrepancy in packet classification between the Fast Ethernet and Gigabit Ethernet interfaces.</p> <p>There are no known workarounds.</p>
CSCsd03740	<p>The <b>cable upstream 0 scheduling type ?</b> command is not synchronized during N+1 switchover.</p> <p>There are no known workarounds.</p>
CSCsd20606	<p>A parallel express forwarding (PXF) restart disables multicast traffic that matches the Multicast Quality of Service (MQoS) configuration.</p> <p>This issue occurs when an MQoS configuration is applied to cable interfaces, and PXF is restarted</p> <p>There are no known workarounds.</p>
CSCsd20683	<p>A command switchover with a virtual interface (VI) configuration is not switching the whole line card.</p> <p>By default, when VI is enabled on an interface, the Hot Standby Connection-to-Connection Protocol (HCCP) line card should switchover the whole line card instead of switching an individual domain.</p> <p>There are no known workarounds.</p>
CSCsd29450	<p>A Protect LC crashes after a sequence of route processor (RP) and LC switchovers.</p> <p>This issue occurs when performing a sequence of LC and Performance Routing Engine (PRE) switchovers.</p> <p>There are no known workarounds.</p>
CSCsd30267	<p>The Authentication, Authorization, and Accounting (AAA) per user process is holding memory, and the router is running out of memory.</p> <p>This issue occurs when PPP over Ethernet (PPPoE) dialing and dynamic access control lists (ACLs) are present.</p> <p>There is no known workaround.</p>
CSCsd31970	<p>On a Cisco uBR10000 series router cable modem termination system (CMTS) with redundant Performance Routing Engine (PRE) modules, new interface mode configuration commands entered on the active PRE may not be properly synchronized to the standby PRE if the <b>do show running-configuration</b> command is entered in interface configuration mode.</p> <p>This issue can lead to a configuration mismatch between the two PRE modules and can cause difficulty on PRE switchover.</p> <p>Workaround: Refrain from issuing the <b>do show running-configuration</b> command in interface configuration mode, or completely exit interface configuration mode after issuing the command.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCsd33394	<p>On Cisco uBR10000 series routers, cable modem termination system (CMTS) upstream subscriber traffic management filters do not filter packets with a multicast destination IP address.</p> <p>Workaround: Configure and apply an IP access-list to the cable or bundle interface that applies to traffic for all the modems and customer premises equipment (CPE) on the interface.</p>
CSCsd36652	<p>When configuring line card redundancy by using the <b>global HA</b> commands, duplicate RF-switch slot numbers were configured. This configuration is not allowed.</p> <p>There are no known workarounds.</p>
CSCsd43741	<p>VID data in the entPhysicalHardwareRev MIB displays the wrong value if the data field in EEPROM is missing.</p> <p>This issue affects the Entity MIB in all Cisco uBR10000 software releases, if the VID data field is not programmed.</p> <p>There are no known workarounds.</p>
CSCsd44373	<p>Certain upstream (US) parameters are not copied from a Working cable line card (CLC) to the Protect CLC during a failover under the following conditions: -upstream docsis mode, -upstream modulation profile, -upstream data-backoff.</p> <p>Because the original settings on the Protect CLC remain, it is possible after a failover to have a Data-over-Cable Service Interface Specification (DOCSIS) mode and modulation profile inconsistent with that of the Working CLC prior to the failover. This inconsistency can create problems. For example, if a Time Division Multiple Access (TDMA)-only Working CLC fails over to a Protect CLC configured with Asynchronous Time Division Multiple Access (ATDMA), the cable modems will switch to ATDMA mode. When the Protect fails back to the TDMA-only Working CLC, the cable modems will continue to use ATDMA and lose IP connectivity.</p> <p>There are no known workarounds.</p>
CSCsd47667	<p>The cable meter feature is causing redundancy to fail between PRE2s due to Inter-Process Communication (IPC) timeouts.</p> <p>This issue occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC2 or 12.3(17a)BC.</p> <p>Workaround: Reload the standby PRE2.</p>
CSCsd65022	<p>The downstream (DS) bandwidth scheduler doesn't work correctly after a PacketCable Multimedia (PCMM) call switchover.</p> <p>There are no known workarounds except to reload the cable modem termination system (CMTS).</p>
CSCsd67236	<p>A policy-based routing (PBR) map with a set clause does not act on matching packets.</p> <p>This issue occurs on PRE1s on Cisco uBR10000 series routers only.</p> <p>There are no known workarounds.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsd73128	A voice call is not fully recovered until 6 seconds after a CLI LC switchover. Workaround: Enter the <b>cable sync-interval 2</b> command on all Working and Protect interfaces before attempting a switchover.
CSCsd77991	A line card on the Cisco uBR10000 series router unexpectedly crashes. This issue occurs when the <b>clear cable modem</b> command is executed for multicast address. Workaround: Do not use the <b>clear cable modem</b> command for multicast addresses.
CSCsd78370	The privacy bit value of the Multicast entries present on the cable modem termination system (CMTS) host database change after a Route Processor Redundancy (RPR) switchover. This issue occurs when adding multicast entries into the CMTS host database but before the RPR Switchover. There are no known workarounds.
CSCsd95113	A cable modem, when enforced with a quality of service (QoS) profile created using the <code>cdxCmtsCmQosProfile</code> MIB, accepts the profile and <b>show cable modem reg</b> shows the modem with the enforced profile. However, the same cable modem, after reset, does not come online with the enforced profile. Instead, it comes online with the default profile. In contrast, the same modem (when enforced with the QoS profile created using the CLI) comes online after reset with the enforced profile, not the default profile. This behavior is the same irrespective of platforms and whether the QoS profile is created using the CLI or the Simple Network Management Protocol (SNMP). There are no known workarounds.
CSCse00902	Various <b>show</b> commands use improper case and spelling. There are no known workarounds.
CSCse02543	When some modems are in the reject state and a <b>clear cable modem reject delete</b> command is issued, a <code>CM_INCONSISTENCY</code> message is generated. Workaround: Do not use the <b>clear cable modem reject delete</b> command.
CSCse08883	After two Performance Routing Engine (PRE) switchovers, a non-functioning High Availability (HA) LC becomes active on the PROTECTA MC520H line card. There are no known workarounds.
CSCse22482	After a Performance Routing Engine (PRE) failover, downstream voice traffic moves from dynamic flow to primary flow. There are no known workarounds.

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCse24904	<p>When a lockout of the Working card is followed by online insertion and removal (OIR), the following two problems occur: 1) OIR switches from the Working card to the Protect card, dropping all the cable modems. 2) After the Working card is back from the OIR, traffic stays on the Protect card with the cable modems down, and the Working card has lockout active. Clearing lockout fails, and because the Working card is standby, reverting to the Working card would also fail.</p> <p>There are no known workarounds.</p>
CSCse25969	<p>The standby Performance Routing Engine (PRE) crashes at cmts_adm_ctrl_bw_init_mschedp_type.</p> <p>The crash occurs only while booting the standby PRE.</p> <p>There are no known workarounds.</p>
CSCse27391	<p>The Hot Standby Connection-to-Connection Protocol (HCCP) stops working properly when a switchover is required from the Working card to the Protect card.</p> <p>No errors are shown. Switching back to the Working card gets the cable modems back online.</p> <p>Workaround: Reload the box; a reload/reseat of the line cards does not work.</p>
CSCse32310	<p>An MC520 crash occurs.</p> <p>There are no known workarounds.</p>
CSCse32901	<p>Overlapping RF switch slots numbers are configured in a global High Availability (HA) 4+1 setup.</p> <p>There are no known workarounds.</p>
CSCse43344	<p>The user can experience bad voice quality, if Low Latency Queueing (LLQ) is configured without enabling Admission Control.</p> <p>This issue occurs when the user configures upstream scheduler mode with LLQ.</p> <p>Workaround: Enable AC after you have configured upstream (US) LLQ.</p>
CSCse45342	<p>Configuring cable default-tos-qos10 tos-overwrite and resetting the modem does not create a new qos-profile. The modem comes online with the existing profile.</p> <p>The problem occurs on modems provisioned in Data-over-Cable Service Interface Specification (DOCSIS) 1.0 mode when the default tos-mask and tos-value are configured.</p> <p>There are no known workarounds.</p>
CSCse48454	<p>Entering a <b>shut/no shut</b> command on an interface triggers infinite switchovers.</p> <p>There are no known workarounds.</p>
CSCse50735	<p>After a cable line card failover, the dynamic Service Flow (SF)-to-Multiprotocol Label Switching (MPLS) virtual private network (VPN) mapping feature no longer works.</p> <p>There are no known workarounds.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCse54378	<p>On a Cisco uBR10000 series router running Cisco IOS image ubr10k-k9p6u2-mz.2006-06-02.123_17_BC, tracebacks are found at sch_rp_download_debug_info when you attempt to configure an already assigned address.</p> <p>There are no known workarounds.</p>
CSCse55592	<p>Two typos exist in the microcode under the Cisco uBR10000 PRE2 platform that can potentially result in some feature errors (including Input/Output ACL, MLP Rx, MLP Tx, MAC Rewrite, and WRED Calc.)</p> <p>There are no known workarounds.</p>
CSCse56676	<p>The cdrqCmtsCmRQDoneNotification trap, which indicates that the cable remote-query function has finished a polling cycle for modems on the cable modem termination system (CMTS), is sent to Simple Network Management Protocol (SNMP) management stations, even when cable specific traps are not configured to be sent to those stations.</p> <p>This condition occurs on a Cisco uBR series CMTS, and can occur on any trap sent, even when the trap is not associated with the SNMP host.</p> <p>There are no known workarounds.</p>
CSCse57637	<p>The Low Latency Queueing (LLQ) upstream scheduler option does not distinguish between Non Real Time Polling Service (nrtPS) and Real Time Polling Service (rtPS) flows correctly.</p> <p>There are no known workarounds.</p>
CSCse64138	<p>When load-balancing is used, some modems might go into init(rc) after an upstream channel change (UCC).</p> <p>There are no known workarounds.</p>
CSCse67808	<p>The cdpCacheTable contains entries with index 4294967295 that are only available using the Simple Network Management Protocol (SNMP) <b>get-next</b> command. When the <b>get-one</b> command is used to retrieve the same value, the NO_SUCH_INSTANCE_EXCEPTION is returned.</p> <p>This issue appears to be related to the management ethernet port on the secondary Performance Routing Engine (PRE) in a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCse67868	<p>The Simple Network Management Protocol (SNMP) cpmCPUTotalPhysicalIndex object returns valid entPhysicalIndex values for cable line cards when these values are retrieved using the <b>getnext</b> command, but when the <b>getone</b> command is used, the physical index values for the cable line cards (CLCs) are returned as 0.</p> <p>This issue occurs on Cisco uBR10000 series routers with CLCs and SNMP configured</p> <p>There are no known workarounds.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCse69641	<p>When the <b>show cable modem s t</b> command is issued soon after a <b>clear cable modem all delete</b> command, the console and vty get stuck.</p> <p>The issue occurs in large-scale environments with more than 5000 modems.</p> <p>Workaround: Do not use the <b>clear cable modem all delete</b> command; delete specific modems instead.</p>
CSCse71725	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>cable monitor</b> command does not successfully monitor upstream bandwidth request messages.</p> <p>There are no known workarounds.</p>
CSCse78143	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>show cr10k-rp cable x/y/z sid</b> command does not allow the service identifier (SID) value to be set to values greater than 8176. As a result, queues associated with downstream multicast quality of service (QoS) SIDs cannot be examined.</p> <p>There are no known workarounds.</p>
CSCse80641	<p>The Transparent LAN Service (TLS) feature does not support stacked dot1q tags.</p> <p>This condition occurs when the TLS feature is configured, and the cable modem termination system (CMTS) receives a 1522 bytes packet (including the frame check sequence (FCS)) in the upstream direction that contains an 802.1q tag.</p> <p>There are no known workarounds.</p>
CSCse81859	<p>On a Cisco uBR10012 router running on Cisco IOS Release 12.3(13a)BC2, the Cisco uBR10-MC5X20U line card crashed with the following error:</p> <pre>Cause 80000010 (Code 0x4): Address Error (load or instruction fetch) exception Crash info file was written and the LC was reloaded</pre> <p>There are no known workarounds.</p>
CSCse82337	<p>The on-board Fast Ethernet board (interface fastethernet 0/0/0) does not recognize that the line protocol is down.</p> <p>This issue occurs after reloading PRE2.</p> <p>Workaround: Enter <b>shut /no shut</b> on the interface, or reload PRE2 again.</p>
CSCse85188	<p>On a Cisco cable modem termination system (CMTS), the quality of service (QoS) profile value for the maximum downstream burst is not displayed correctly and may not be set correctly after a reload.</p> <p>This issue occurs when the maximum downstream burst for a QoS profile is configured using the <b>cable qos profile n max-ds-burst value</b> command with a <i>value</i> greater than 2147483647. The value will be displayed as a negative number in the <b>show run</b> command output. If the configuration is written to memory, the maximum downstream burst is also saved as a negative number. As a result, this value is not processed correctly when the configuration is processed after a reload.</p> <p>There are no known workarounds. (Note that the <b>cable qos profile</b> command has been deprecated for Data-over-Cable Service Interface Specification (DOCSIS) 1.1 use because DOCSIS 1.1 replaces the QoS profile with a service flow, which is configured using the <b>cable service class</b> command.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCse86436	<p>Massive Embedded Media Terminal Adapter (eMTA) flapping occurs after long hours of more than 1000 PacketCable Multimedia (PCMM) calls. All flapping eMTAs re-register back.</p> <p>There are no known workarounds.</p>
CSCse86458	<p>Many Arris Embedded Media Terminal Adapters (eMTAs) on an Asynchronous Time Division Multiple Access (ATDMA) channel go offline after an MC520u CLI switchover with PacketCable calls.</p> <p>There are no known workarounds.</p>
CSCse88914	<p>The total of exclusive bandwidth allocated to various service class names of a particular scheduling type exceeds the exclusive allocation configured for that scheduling type.</p> <p>There are no known workarounds.</p>
CSCse97227	<p>The cable modem termination system (CMTS) crashes while un-configuring global Hot Standby Connection-to-Connection Protocol (HCCP) configurations.</p> <p>This issue occurs only when the global HCCP configuration includes slot numbers that are not present in the CMTS.</p> <p>There are no known workarounds.</p>
CSCse98224	<p>About 10 minutes after loading Cisco IOS Release 12.3(17a)BC2 on a Cisco uBR10000 series router with about 5000 cable modems and digital set-top boxes (STBs) connected, the operator was unable to ping to directly connected Backbone Switches' interfaces on the Cisco uBR10000 series router, and the Open Shortest Path First (OSPF) neighbor with the Backbone Switches (OSRs) was in the DOWN state. The Gigabit Ethernet interfaces' state was UP, and the only log message to appear was that the OSPF neighbor's state was down.</p> <p>There are no known workarounds.</p>
CSCse99462	<p>Spurious Accesses traceback occurs. The static Hot Standby Connection-to-connection Protocol (HCCP) sync keeps sync, but is not able to resolve, because the STATICSYNCDONE is not received,</p> <p>This issue occurs in an N+1 global configuration, after the line card switchover but before the sync is completed, and when flapping one port of Protected interface (in the HCCP active state)</p> <p>Workaround: Do not flap the HCCP active interface before the sync completes.</p>
CSCsf00801	<p>Internet Control Message Protocol (ICMP) packets are captured on the cable monitoring interface where they shouldn't be replicated when the cable monitor interface FastEthernet0/0/0 access-list [2] [packet-type ethernet] is configured on the cable line card.</p> <p>This issue can occur both upstream and downstream, and regardless of access list type: numbered, named, standard or extended.</p> <p>There are no known workarounds.</p>
CSCsf02972	<p>When moving upstreams with more than 500 cable modems to an upstream port on the Cisco uBR10000 series router, some modems do not come online.</p> <p>Workaround: Change the upstream frequency to get them to come online.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsf02982	<p>When an attempt is made to modify the in-use Peer-to-Peer (P2P) policy, an error occurs.</p> <p>There are no known workarounds.</p>
CSCsf04338	<p>The Cisco uBR series cable modem termination system (CMTS) with cable or bundle subinterfaces configured does not prevent customer premises equipment (CPE) from receiving a Dynamic Host Configuration Protocol (DHCP) offer with an IP address belonging to the wrong subinterface. Only DHCP offers that contain an offered IP address within the same subinterface as the cable modem belonging to the customer premises equipment (CPE) should be forwarded by the CMTS.</p> <p>The issue occurs when the CMTS is configured to use cable or bundle subinterfaces and the DHCP server is wrongly configured.</p> <p>Workaround: Ensure that the DHCP server is configured to assign CPE devices IP addresses from only the appropriate IP subnets.</p>
CSCsf07848	<p>On a Cisco uBR series cable modem termination system (CMTS), the Embedded Media Terminal Adapter (eMTA) component of a PacketCable enabled device cannot get IP connectivity if another customer premises equipment (CPE) device in the system has previously used the MAC address of the eMTA.</p> <p>Workaround: Issue the clear cable host affected-mac-address command to release control of the affected mac address and to allow the eMTA to take ownership of that MAC-address.</p>
CSCsf10689	<p>For some cable upstream interfaces, no entry exist in the DOCS-IF-MIB and the CISCO-CABLE-SPECTRUM-MIB.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.2(15)BC2e and Cisco IOS Release 12.2(15)BC5.</p> <p>There are no known workarounds.</p>
CSCsf12149	<p>While deleting the second stream intercept, the Simple Network Management Protocol (SNMP) returns with a COMMIT_FAILED_ERROR. The <b>getmany</b> command shows that the stream is actually deleted.</p> <p>This issue occurs when each stream has a different protocol value, each stream is associated with different MD, and an attempt is trying to delete the second stream.</p> <p>Workaround: Ignore the error message; the stream is actually deleted.</p>
CSCsf18311	<p>An RF line card failover occurs as a result of powering down the Working line card.</p> <p>There are no known workarounds.</p>
CSCsf19110	<p>In a large-scale setup with more than 5000 modems, if you copy a baseline privacy interface (BPI)- enabled configuration file and enter the <b>clear cable modem all del</b> command, after at least 4000 modems are up, tracebacks and memory alloc failure messages are found on the MC520u cards.</p> <p>There are no known workarounds.</p>
CSCsf22037	<p>The cable sflog maximum entry value needs to be changed to 1-59999</p> <p>There are no known workarounds.</p>

**Table 71** Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)

DDTS ID Number	Description
CSCsf27296	<p>If two line cards failover to the Protect card at the same time, the Performance Routing Engine (PRE) can crash/ failover shortly afterwards. While a majority of the modems recover, some get stuck from init(rc) to init(o).</p> <p>This issue occurs on a Cisco uBR10000 series router with PRE2, MC520s, and MC520u cards running Cisco IOS Release 12.3(9a)BC8.</p> <p>Workaround: Try resetting the PRE, or resetting Parallel Express Forwarding (PXF) through the CLI.</p>
CSCsf29154	<p>The communication between the line cards and the routing processor fails. The output of <b>show diag</b> command is empty.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC1.</p> <p>Workaround: Reload the router.</p>
CSCsf30877	<p>The wrong classification is applied to the IP Protocol field.</p> <p>There are no known workarounds.</p>
CSCsf31242	<p>The <b>show cable modem cpe_ip</b> command should display information about the cable modem with which a customer premises equipment (CPE) device is associated, but does not.</p> <p>This issue is seen on one cable modem termination system (CMTS), multiple line cards, and multiple upstream/downstreams. This issue recurs intermittently, a few times a month, with no known cause.</p> <p>Workaround: Enter the <b>clear cable modem delete</b> command to work around the issue.</p>
CSCsf31762	<p>Some packets may not be dequeued from a cable interface, causing the input queue size to increase beyond the maximum configured queue size. As a result, traffic drops and modems go offline.</p> <p>This issue occurs on the 5cable-MC520s-d card on the Cisco uBR 10k platform, and appears to be caused by a particular (possibly corrupted) packet.</p> <p>Workaround: Increase the queue size using the <b>hold-queue</b> command to temporarily fix the problem.</p>
CSCsf33128	<p>All the wideband cable modems in the cable modem termination system (CMTS) reset when a configuration file is uploaded from disk to become the running configuration. All the modems return online after the reset and function properly.</p> <p>This issue occurs only when spectrum management has been configured in the configuration file.</p> <p>Workaround: Remove the spectrum management configuration from the configuration file.</p>
CSCsf96635	<p>The following error message, followed by a traceback occurs on the router after a period of normal operation:</p> <pre>%GENERAL-3-EREVENT: HWCEF: Loadinfo fastadj lock with NULL fasttag_rew</pre> <p>There are no known workarounds.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsf98118	<p>A buffer leak in the small buffer occurs on cable routers. The <b>show buffers</b> command shows the small buffers increasing in the total buffers, and the <b>show process cpu</b> command shows that the IP Input process is holding more and more memory.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(17a)BC.</p> <p>There are no known workarounds.</p>
CSCsf99847	<p>A Cisco uBR10000 series router running ubr10k-k8p6-mz.123-9a.BC9 crashes with an unexpected exception, CPU signal 23: "%SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 63AD71B0, data B0D0B0D"</p> <p>There are no known workarounds.</p>
CSCsg03719	<p>Tracebacks and spurious memory accesses occur after a Performance Routing Engine (PRE) switchover.</p> <p>This issue occurs in a large-scale testbed with more than 5000 modems.</p> <p>There are no known workarounds.</p>
CSCsg16433	<p>The mac-address in the metering file is wrong. Instead of the management interface address it shows the mac-address of the first interface in the <b>show ip interface brief</b> list.</p> <p>There are no known workarounds.</p>
CSCsg16781	<p>A stream cannot be configured with a source IP address whose subnet is not in the cable modem termination system (CMTS).</p> <p>Workaround: Try to configure a stream from subnet which is present on the CMTS.</p>
CSCsg17050	<p>The DOCSIS Set-Top Gateway (DSG) interface configuration is not retained when a 5X20S card is replaced with a 5x20U card, and vice versa.</p> <p>Workaround: Remove the dsg tg configuration from the global configuration, configure it again, and apply the configuration to the interface.</p>
CSCsg17576	<p>The Cisco uBR10012 MC520u upstream PHY TI4522 receiver does not work correctly with the Data-over-Cable Service Interface Specification (DOCSIS) 2.0 Reed Solomon dynamic interleaver.</p> <p>When a customer creates a modulation profile that includes Asynchronous Time Division Multiple Access (ATDMA) interval usage code (IUC) values, such as A-LONG, with dynamic interleaver enabled it can cause the upstream port to lose data over time for the ATDMA modems and can also cause the signal-to-noise ratio (SNR) reported for those upstreams to report very poor SNR values minutes after traffic passes on those ports.</p> <p>Workaround: Ensure your modulation profile does not have dynamic interleaver enabled for any A-DMA IUC elements, such as A-LONG or A-UGS.</p>
CSCsg21610	<p>If the minimum information rate (MIR) of a service flow is specified as zero (or unspecified) and best effort service flow policing is enabled, the best effort service flow rate is limited to 64Kbps.</p> <p>Workaround: Specify an MIR value for best effort service flows.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCsg25638	<p>An MC520u line card in a Cisco uBR10000 cable modem termination system (CMTS) spontaneously reloads.</p> <p>This issue occurs on a CMTS running Cisco IOS Release 12.3(9a)BC7.</p> <p>There are no known workarounds.</p>
CSCsg27690	<p>A traceback is generated if the card configuration that is the upper slot of an Spatial Reuse Protocol (SRP) card pair is removed (no card) from the running configuration while the SRP interface has an output service policy applied.</p> <p>Workaround: If the service policy is removed from the SRP interface prior to the upper slot card being un-configured, the traceback is not generated.</p>
CSCsg30121	<p>If the <b>debug cable mac-address</b> command is enabled and the cable monitor is configured, <b>cable monitor debug</b> outputs flood the console.</p> <p>This issue occurs even if the debug and cable monitor commands are for different devices. The amount of these packets generated can be very large and can be a great annoyance on the console.</p> <p>There are no known workarounds.</p>
CSCsg31641	<p>After a switchover between Performance Routing Engines (PREs), the Transparent LAN Service (TLS) stops passing traffic to the Gigabit Ethernet interface until another switchover occurs. (The TLS configuration remains identical on both PREs before and after the switchover.)</p> <p>This issue is specific to the Half-Height Gigabit Ethernet (HHGE) line card and occurs as a result of a redundancy switchover and a Gigabit Ethernet interface reset.</p> <p>Workaround: Remove the TLS configuration on the active PRE and then re-add it again.</p>
CSCsg32252	<p>A Cisco uBR10-MC5X20U card reports an impossibly low upstream (US) signal-to-noise ratio (SNR) for Quadrature Amplitude Modulation 16 (QAM16) with some working cable modems. However, the affected subscribers do not report any problems.</p> <p>Reportedly, the problem was not seen before the hardware upgrade from MC28/UBR7200 to MC5x20/UBR10K.</p> <p>Workaround: Rely on the error counters, rather than on the SNR readings.</p>
CSCsg34038	<p>The ifDescr Snmp query returns a negative value when the subinterface bundle is configured with the maximum subinterface number allowed.</p> <p>Workaround: Do not configure the maximum subinterface number when configuring the subinterface bundle.</p>
CSCsg38426	<p>In a system with 40 virtual interface bundles, assigning one of those virtual interface bundles to all mac domains in a fully loaded chassis, generates the following message on the console after deleting the assigned virtual interface bundle:</p> <pre>*MCASTECHO: All DS Group Index has been used up. Interface: Cable6/1/4 VCCI:: 33.</pre> <p>There are no known workarounds.</p>

**Table 71**      **Open Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCsg39288	<p>Backup TCC card may experience a reload (IPCOIR-3-TIMEOUT on TCC card). The issue has been experienced on 12.3(9a)BC9, 12.3(13a)BC2 and 12.3(13a)BC6. There are compare errors in the <b>show controllers clock-reference</b> that do increment. However the clocks are not actually drifting apart, even though the errors are incrementing. Because clocks are not actually drifting, redundancy is not affected, except during the brief period when the backup TCC+ card reloads after a IPCOIR timeout.</p> <p>There are no known workarounds.</p>
CSCsg39990	<p>Cable filter groups do not filter local traffic on the Cisco uBR10000 series platform.</p> <p>There are no known workarounds.</p>
CSCsg44938	<p>A swap between the MC520H card and MC520u card forces the first JIB's downstreams into the shutdown state. For instance, if you downgrade from the MC520H card to the MC520u card, the MC520u card will shutdown Cx/y/0 and Cx/y/2 to build its configuration.</p> <p>This issue occurs on a Cisco uBR10000 series router running an interface-level Hot Standby Connection-to-Connection Protocol (HCCP) configuration on Cisco IOS Release 12.3(17a)BC2, with the <b>cr10k card slot/subslot oir-compatibility</b> command enabled.</p> <p>There are no known workarounds.</p>
CSCsg45576	<p>The router can unexpectedly restart during line card online insertion and removal (OIR) if the execution of the <b>show pxf cpu queue</b> command is preempted by the <b>More</b> prompt, and the command output is allowed to continue after the line card has fully initialized.</p> <p>Workaround: Allow the command output to complete before performing an OIR of the associated line card.</p>
CSCsg45624	<p>Unexpected downstream packet loss occurs within the 5x20H Cable line card during periods of congestion.</p> <p>Workaround: There are no known workarounds with the exception of trying to prevent the congestion from occurring.</p>
CSCsg45692	<p>The Cisco uBR10K 5X20 line card crashes at <code>cr10k_clc_pre_poll</code>.</p> <p>This issue occurs on Cisco IOS Release 12.3(13a)BC6 or Cisco IOS Release 12.3(9a)BC7.</p> <p>There are no known workarounds.</p>
CSCsg46284	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC6 may not generate a crashinfo file for the uBR10K-MC5x20U-D line card.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(17b)BC3

Table 72 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17b)BC3.

**Table 72** Resolved Caveats for Cisco IOS Release 12.3(17b)BC3

DDTS ID Number	Description
CSCeb54486	<p>A Cisco uBR10012 router running Cisco IOS Release 12.2(11)BC3, PRE A crashed due to a bus error, but the active Performance Routing Engine (PRE) didn't switchover to PRE B.</p> <p>Workaround: Do not execute the <b>show snmp sessions</b> command.</p>
CSCee00642	<p>After performing a <b>wr erase</b>, followed by a reload, the PRE2 crashes.</p> <p>There are no known workarounds.</p>
CSCee27341	<p>A Cisco uBR10012 router experiences a software-forced crash (memory corruption in snmp) after executing the following command:</p> <pre>no snmp-server host xx.xx.xx.xx public</pre> <p>There are no known workarounds other than not using the <b>no snmp-server host</b> command.</p>
CSCee39660	<p>The cable modem termination system (CMTS) reports a traceback error during a Performance Routing Engine (PRE) switchover.</p> <p>There are no known workarounds.</p>
CSCeh48889	<p>The INVALIDSIDPOSITION message occurs on an interface when a large number of cable modems are going online and offline at once</p> <p>For example:</p> <pre>%UBR10000-3-INVALIDSIDPOSITION: Invalid SID (4184) position for interface Cable5/0/0: CM 00d1.1477.7451:Is used by CM 00d0.d726.ef0b SFID 6813 SID 4184. SID container info: start 744 end 6967 -Traceback= 6030A628 6030A844 6030B098 602F81FC 603A480C 605E1398 605E137C</pre> <p>One typical trigger for this message is the <b>clear cable modem delete</b> or <b>clear cable modem oui oui delete</b> command. The affected modem is kicked offline and will usually come back online later. Many different modems may be affected.</p> <p>Workaround: <b>Shut /no shut</b> the affected cable interface, or delete most modems on the cable interface.</p> <p>Alternative workaround: Reduce the number of cable modems on the affected cable interface by moving modems to other ports.</p>

**Table 72 Resolved Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCei93982	<p>The router crashes unexpectedly because of Network Address Translation (NAT) source and destination port handling.</p> <p>This issue occurs when NAT is enabled and an application uses two well-known ports: one for the source and the other for destination. The outgoing translation is created, but on the return trip, because NAT is using the previous source port as the destination, NAT may use the incorrect algorithm. For example, if a Point-to-Point Tunneling Protocol (PPTP) session is initiated to the well-known port 1723 from source port 21 for the File Transfer Protocol (FTP), then the outgoing packet will create an FTP translation (because source information is examined in the outgoing direction). When the packet is returned, the source information is examined again to determine its packet type. In this case, because the source port is 1723, NAT assumes this is a PPTP packet and attempts to perform PPTP NAT operations on the data structure that NAT built for an FTP packet. This condition can lead to a router crash.</p> <p>There are no known workarounds.</p>
CSCek26492	<p>Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability: <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-ip-option">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-ip-option</a></p> <p>Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.</p> <p>Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information: <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-ip-option">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-ip-option</a></p>
CSCek39658	<p>The value of cable modemTipAddress in the IP Detail Record (IPDR) information, sent by the cable modem termination system (CMTS) when cable billing is configured is currently set to the lowest IP address numerical value on the CMTS. This value is not guaranteed to be consistent for a given CMTS.</p> <p>There are no known workarounds.</p>
CSCek48359	<p>Frequent line card crashes occur at the cable modem termination system (CMTS) due to memory corruption.</p> <p>There are no known workarounds.</p>
CSCek49340	<p>When the gate-id is greater than 8388608, and the line card is rebooted for any reason, the line card gets stuck in recursive crashes.</p> <p>This issue occurs after long hours of bulk PacketCable and PacketCable Multimedia (PCMM) calls (totalling more than 1100 calls).</p> <p>Workaround: Reload the cable modem termination system (CMTS).</p>

Table 72 Resolved Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)

DDTS ID Number	Description
CSCek50191	<p>When configuring a cable modem with the ACL option, the cable modem termination system (CMTS) flushes out traceback and spurious memory access.</p> <p>There are no known workarounds.</p>
CSCek52589	<p>The following extensible markup language (XML) elements, created by a router configured to run the Subscriber Account Management Interface Specification (SAMIS), do not conform to the IPDR 3.5-A.0 format:</p> <ul style="list-style-type: none"> <li>• CMTShostname should be CMTShostName (uppercase N).</li> <li>• CMdocsisMode should report values as either 10, 11 or 20 rather than 1.0, 1.1 and 2.0. (no dots).</li> <li>• Rectype should be RecType (uppercase T).</li> </ul> <p>There are no known workarounds.</p>
CSCin92949	<p>When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.</p> <p>This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.</p> <p>Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.</p>
CSCsc36824	<p>A Cisco router may reload unexpectedly due to a bus error exception. The crashinfo shows a translational bridging (TLB) (load or instruction fetch) exception.</p> <p>This condition occurs with Network Address Translation (NAT) H.323 slow start calls.</p> <p>Workaround: The unexpected reload does not occur when using H.323 FastStart.</p>
CSCsc52024	<p>Interface throughput can be reduced when an output service policy is removed.</p> <p>This issue occurs if the service policy being removed defines a bandwidth percentage on the class-default.</p> <p>There are no known workarounds.</p>
CSCsc78813	<p>While using Network Address Translation (NAT) in an overlapping network configuration, the IP address inside a Domain Name System (DNS) reply payload from the name server is not translated at the NAT router.</p> <p>This condition occurs on a Cisco router that runs Cisco IOS Release 12.3(18) and that has their <b>nat outside source</b> command enabled. The condition can also occur in Cisco IOS Release 12.4 or Cisco IOS Release 12.4T.</p> <p>There are no known workarounds.</p>
CSCsc90295	<p>A Cisco UBR10000 PRE1 may unexpectedly reload due to a bus error when running Cisco IOS Release 12.3(13a)BC1.</p> <p>There are no known workarounds.</p>

**Table 72**      **Resolved Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCsd27514	<p>Traffic on service flows with a non-zero Traffic Priority value are treated as zero priority.</p> <p>This issue occurs if there is a restart of parallel express forwarding (PXF) while the non-zero priority service flows are present.</p> <p>Workaround: Reset the affected modem.</p>
CSCsd58381	<p>Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.</p> <p>Cisco has made free software available to address this vulnerability for affected customers.</p> <p>There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-IOS-IPv6">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-IOS-IPv6</a></p>
CSCsd59817	<p>On the MC520u card signal-to-noise ratio (SNR) values may drop on the upstream, which can cause modems to drop offline.</p> <p>This issue occurs on Cisco uBR10000 series routers running Cisco IOS Release 12.3(9a)BC8 with multiple MC520u cards.</p> <p>Workaround: Either disable/enable pre-equalization on the upstream, or change the modulation on the upstream.</p>
CSCsd95828	<p>Telnet or Secure Shell (SSH) access to the Cisco uBR10000 series router fails after a Performance Routing Engine (PRE) switchover/failover.</p> <p>This issue occurs on Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC3 with a line vty configured for "login local" on the active PRE.</p> <p>Workarounds: Either configure a password under the line vty, or configure Authentication, Authorization, and Accounting (AAA) authentication as follows:</p> <pre>Router#conf term Enter the following configuration commands, one per line. End with <b>Control-Z</b>. Router(config)#aaa new-model Router(config)#aaa authentication login ABC local Router(config)# Router(config)#line vty 0 4 Router(config-line)#login authentication ABC</pre>

**Table 72 Resolved Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCsd96270	<p>Parallel express forwarding (PXF) crash info files are missing a portion of the PXF direct memory access (DMA) information.</p> <p>This issue occurs after a restart of PXF; if a crashinfo file is requested, the file is missing this information.</p> <p>There are no known workarounds.</p>
CSCsd97968	Support for additional error checking was added to the code.
CSCse02868	<p>A spurious memory access error occurred involving if-cons to cable line card slots and a Performance Routing Engine (PRE) failover.</p> <p>There are no known workarounds.</p>
CSCse05641	<p>Syslog messages with new lines get truncated on the syslog server and are treated as invalid.</p> <p>This issue occurs because the system event message has message-text with a new line (\n), causing the message to be in two lines rather than a single line.</p> <p>As a result, the message appears in the cable modem termination system (CMTS) logs in separate lines:</p> <pre>Apr 17 15:01:22.489 EDT: %UBR10000-3-MACADDRERR: DHCP Msg with non unicast MAC address. Master Interface Cable7/0/0 Input Interface SID = 65535 MAC = 0000.0000.0000</pre> <p>Ideally, the message should be in one line:</p> <pre>Apr 17 15:01:22.489 EDT: %UBR10000-3-MACADDRERR: DHCP Msg with non unicast MAC address. Master Interface Cable7/0/0 Input Interface SID = 65535 MAC = 0000.0000.0000</pre> <p>There are no known workarounds.</p>
CSCse24179	<p>The dynamic service flow created for PacketCable Multimedia (PCMM) sessions for the Speed Preview application hangs.</p> <p>Workaround: Because the Speed Preview application cannot set the PCMM T3 timer (DOCSIS T8 timer), the only way to clean up the service flow is to identify the flows that are stuck and enter the <b>test cable dsd ip-addr-of-modem</b> command.</p>
CSCse25429	<p>While netbooting the cable modem termination system (CMTS) with the latest geo_cable image, the CMTS crashes.</p> <p>This issue occurs when CMTS has unsupported DOCSIS Set-Top Gateway (DSG)1.2 configurations on the startup at the time of netbooting.</p> <p>Workaround: Load the image without having any unsupported DSG configurations on the startup.</p>
CSCse28069	<p>High CPU usage in the TTY background occurs on a terminal server connected to a Cisco uBR10000series router (PRE2) when the <b>modem inout</b> command is configured.</p> <p>Workaround: Disable the <b>modem inout</b> command.</p>
CSCse32240	<p>When load balancing is configured and an upstream channel change (UCC) request is sent to, but not answered by, the remote cable modem, the UCC request is not resent.</p> <p>There are no known workarounds.</p>

**Table 72 Resolved Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCse39194	<p>Unencrypted traffic, such as broadcast Address Resolution Protocol (ARP) requests, can leak into an Layer 2 (L2) virtual private network (VPN) supported by a Cisco cable modem termination system (CMTS).</p> <p>There are no known workarounds.</p>
CSCse42277	<p>Configuring a new High Availability (HA) Working line card on the cable modem termination system (CMTS) causes the standby Performance Routing Engine (PRE) to crash if the RF switch name cannot be resolved by the Domain Name System (DNS).</p> <p>Workaround: Verify that the RF switch name can be resolved by DNS before adding the Working line card.</p>
CSCse44203	<p>The <b>show cable leasequery-filter interface requests-filtered</b> command is not updated when upstream threshold=0.</p> <p>There are no known workarounds.</p>
CSCse48188	<p>After a Performance Routing Engine (PRE failover), the dynamic service flow to Multiprotocol Label Switching (MPLS) virtual private network (VPN) feature no longer works.</p> <p>There are no known workarounds.</p>
CSCse50424	<p>On a Cisco uBR10000 series router, PRE2 is experiencing high CPU usage and crashes when querying the customer premises equipment (CPE) (40 CPEs) by the Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCse52836	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), the first cable modem online in a modem created Data-over-Cable Service Interface Specifications (DOCSIS) 1.0 QoS profile may not have its ToS byte correctly overwritten when the <b>cable default-tos-qos10 tos-overwrite</b> command is implemented.</p> <p>There are no known workarounds.</p>
CSCse55926	<p>Modems get stuck in init(o) when upgrading from Cisco IOS Release 12.3(9a)BC9 to Cisco IOS Release 12.3(17a)BC1.</p> <p>When you first upgrade, and the configuration is upgraded from the Cisco IOS Release 12.3 (9a)BC9 to Cisco IOS Release 12.3 (17a)BC1 configuration, all modems get stuck in init(o). They remain stuck in init(o) until you either enter the <b>write memory</b> command and reload the box, or you reload the active Parallel Express Forwarding (PXF).</p> <p>Workaround: Enter the <b>write memory</b> command after upgrading and then reload the router, or reload the PXF.</p>

**Table 72**      **Resolved Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCse65266	<p>Bandwidth calculations for upstream request polls for Real Time Polling Service (rtPS) and Non Real Time Polling Service (nrtPS) service flows can be incorrectly calculated depending on the modulation profile and Data-over-Cable Service Interface Specifications (DOCSIS) mode. It appears that the bps calculation is made based on the settings for the long (or a-long in DOCSIS 2.0 mode) interval usage code (IUC), instead of the request IUC. In Time Division Multiple Access (TDMA)-only mode with a pure Quadrature Phase-Shift Keying (QPSK) or Quadrature Amplitude Modulation 16 (QAM16) environment, this miscalculation is not a problem as request and long IUC are the same with respect to byte size per minislot size. However, when a mixed modulation profile or a mixed/Asynchronous Time Division Multiple Access (A-TDMA)-only mode DOCSIS upstream channel is used, the service flow's reserved bandwidth is greater than what is used or needed. As a result, Admission Control is inaccurate, resulting in fewer permitted service flows and voice calls. Cisco IOS should report the total bps bandwidth consumption of rtPS and nrtPS flows, based on the true size of the request IUC, and not that of the largest IUC (long or a-long).</p> <p>There are no known workarounds.</p>
CSCse66329	<p>The router may reload unexpectedly upon execution of the <b>show pxf cpu qos</b> command with a non-cable interface specified.</p> <p>Workaround: If this command must be executed, ensure that a cable interface is specified.</p>
CSCse68138	<p>The router reloads due to fragmented Resilient Transport Protocol (RTP) packets. This condition is platform-independent, and is most likely to occur in networks where the Voice over IP (VoIP) application is being used and one more segments of the network are using a low maximum transmission unit (MTU).</p> <p>There are no known workarounds.</p>
CSCse77306	<p>You cannot get Simple Network Management Protocol (SNMP) MIB information correctly due to an ifindex problem after an Hot Standby Connection-to-Connection Protocol (HCCP) and Performance Routing Engine (PRE) switchover.</p> <p>Workaround: Issue the <b>cable upstream max-ports x</b> command under the affected cable interfaces, or reload PRE</p>
CSCse92109	<p>The cable modem termination system (CMTS) hangs and then crashes when configuring the <b>ip igmp static-group</b> command at a virtual bundle interface.</p> <p>There are no known workarounds.</p>

**Table 72 Resolved Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCse98768	<p>When attempting to bring up a secondary Performance Routing Engine (PRE) on a Cisco uBR10012 router, a problem occurs creating the startup-configuration file on the secondary PRE. Also, if the <b>auto-sync standard</b> or <b>auto-sync startup-config</b> commands are issued, the following error can appear: % Secondary config compress IOCTransparent LAN Service (TLS) failed.</p> <p>This issue occurs when the monitor environment variable, CONFIG_FILE, does not exist on the primary PRE, which causes the wrong value to be synchronized to the secondary PRE. After a <b>write memory</b> or <b>auto-sync standard</b> command, the secondary PRE attempts to write the startup configuration to disk0, using the bad CONFIG_FILE variable as the filename. Calls to set the compression size fail because the flash file system doesn't support those functions. As a result of the failure, the file is not written; an error message is generated if the <b>auto-sync</b> command triggered the configuration sync.</p> <p>Workaround: Ensure that the secondary PRE is not running, and force the CONFIG_FILE variable on the primary PRE to be defined and null so that the correct value is sent to the secondary PRE when it comes up.</p>
CSCsf04754	<p>Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.</p> <p>The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.</p> <p>Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.</p> <p>This advisory will be posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080610-snmv3">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080610-snmv3</a></p>
CSCsf05280	<p>Only one downstream reports IfCmtsChannelUtUtilization data although the CLI shows traffic on the other downstreams.</p> <p>This issue occurs on a Cisco uBR10000 series router with a uBR10-MC5X20U-D card, running either Cisco IOS Release 12.3(15a)BC5 or Cisco IOS Release 12.3(15a)BC6.</p> <p>There are no known workarounds.</p>
CSCsf13469	<p>When optical cables are pulled out and in several times within a 10 to 12 second interval, the time for the link to come back up can be as long as 4 to 10 minutes.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC1/2/3 or Cisco IOS Release 12.3(17a)BC1. When this issue occurs, the Half-Height Gigabit Ethernet (HHGE) line card stays in the down/down state, and the router stays in the up/down state.</p> <p>There are no known workarounds.</p>

**Table 72 Resolved Caveats for Cisco IOS Release 12.3(17b)BC3 (continued)**

DDTS ID Number	Description
CSCsf14855	<p>Cisco uBR10000 series routers can restart due to memory corruption</p> <p>This issue occurs on Cisco IOS Releases 12.3(17a)BC1, 12.3(17a)BC2 and 12.3(13a)BC6.</p> <p>Workaround: Use Cisco IOS Release 12.3(9a)BC6 when possible.</p>
CSCsf27052	<p>A Cisco uBR10000 series router configured with the Dynamic Message Integrity Check (DMIC) feature crashes.</p> <p>This issue occurs on Cisco IOS Release 12.3(17a)BC1 when DMIC is configured.</p> <p>Workaround: Disable the DMIC feature.</p>
CSCsg04497	<p>A Cisco uBR router that is being upgraded, crashes at bootup due to Init stack overflow corruption.</p> <p>This issue occurs when router has numerous cable interfaces with bundles configured on the initial version, and the router is being upgraded to a new version of Cisco IOS that uses virtual bundling and Open Shortest Path First (OSPF).</p> <p>Workaround: Remove OSPF from the configuration before performing the upgrade and then add OSPF back in after the upgrade.</p>
CSCsg18882	<p>When creating cable modem termination system (CMTS) modulation profiles using the auto generation method <b>cable modulation xxx robust-xxx-xxx</b> command, the dynamic interleaver is set to ON, instead of OFF. This condition can cause packet loss and poor signal-to-noise ratio (SNR) reporting on the CMTS.</p> <p>Workaround: Ensure dynamic interleaver is set to OFF while the modulation profile is in use.</p>

## Open Caveats for Release 12.3(17a)BC2

Table 73 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17a)BC2.

**Table 73 Open Caveats for Cisco IOS Release 12.3(17a)BC2**

DDTS ID Number	Description
CSCeb54486	<p>A Cisco uBR10012 router running Cisco IOS Release 12.2(11)BC3, PRE A crashed due to a bus error, but the active Performance Routing Engine (PRE) didn't switchover to PRE B.</p> <p>Workaround: Do not execute the <b>show snmp sessions</b> command.</p>
CSCee00642	<p>After performing a <b>wr erase</b>, followed by a reload, the PRE2 will crash.</p> <p>There are no known workarounds.</p>
CSCee27341	<p>A Cisco uBR10012 router experiences a software-forced crash (memory corruption in snmp) after executing the following command:</p> <pre>no snmp-server host xx.xx.xx.xx public</pre> <p>There are no known workarounds other than not using the <b>no snmp-server host</b> command.</p>

**Table 73 Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCee39660	<p>The cable modem termination system (CMTS) reports a traceback error during a Performance Routing Engine (PRE) switchover.</p> <p>There are no known workarounds.</p>
CSCef66578	<p>The output of the <b>show cable modem connectivity</b> command displays an extremely large value.</p> <p>This issue occurs in Cisco IOS Releases 12.2(15)BC2b and 12.2(15)BC2c.</p> <p>There are no known workarounds.</p>
CSCeh48889	<p>The INVALIDSIDPOSITION message occurs on an interface when a large number of cable modems are going online and offline at once</p> <p>For example:</p> <pre>%UBR10000-3-INVALIDSIDPOSITION: Invalid SID (4184) position for interface Cable5/0/0: CM 00d1.1477.7451:Is used by CM 00d0.d726.ef0b SFID 6813 SID 4184. SID container info: start 744 end 6967 -Traceback= 6030A628 6030A844 6030B098 602F81FC 603A480C 605E1398 605E137C</pre> <p>One typical trigger for this message is the <b>clear cable modem delete</b> or <b>clear cable modem oui oui delete</b> command. The affected modem is kicked offline and will usually come back online later. Many different modems may be affected.</p> <p>Workaround: <b>Shut /no shut</b> the affected cable interface, or delete most modems on the cable interface.</p> <p>Alternative workaround: Reduce the number of cable modems on the affected cable interface by moving modems to other ports.</p>
CSCei22859	<p>The secondary service does not pass traffic after a line card switchover.</p> <p>This issue is likely related to payload header suppression (PHS) traffic and switchovers.</p> <p>Workaround: Do not use PHS.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are being forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks are observed and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>
CSCej52423	<p>The wrong number of bytes are suppressed and packet drops occur on the dial shelf controller (DSC) when adding payload header suppression (PHS) and line card (LC) switchover.</p> <p>This issue occurs when performing a switchover while using LC redundancy and Multiple PHS for a secondary service flow (SF).</p> <p>Workaround: Do not use PHS with multiple rules for an SF if you are using N+1.</p>

**Table 73**      **Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCek20675	Support is added for the <b>show pxf cable source-verify</b> command for PRE2. There are no known workarounds.
CSCek21720	Traceback occurs with packet intercept during a line card (LC) switchover in PRE2.  This issue occurs when the LC switchover is performed while PacketCable (PC) calls and class features are in progress.  There are no known workarounds
CSCek23320	Simple Network Management Protocol (SNMP)-related traceback is seen when the image is loaded with the attached cable modem termination system (CMTS) configuration:  *Dec 21 16:11:28.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/1, changed state to up Dec 21 16:12:08.141: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61156234 reading 0x0 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 61156234 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 6115623C 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:14:11.138: %AAAA-3-DROPACCTSNDFAIL: Accounting record dropped, send to server failed: system-start There are no known workarounds.
CSCek24075	Zero nodes are reported in the <b>show srp topology</b> command. There are no known workarounds.
CSCek27678	The <b>show access-lists</b> command displays the access control lists (ACLs) for deleted packet filter groups. The corresponding internal ACLs are not removed, even after the packet filter group is deleted.  In addition, the <b>show cable filter</b> command lists the reserved ACL group 255 index 1 with drop action, even if all the cable filter configurations have been removed from the cable modem termination system (CMTS).  There are no known workarounds.

**Table 73** Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)

DDTS ID Number	Description
CSCek29193	<p>Swapping unlike MC520 line cards (s, u) causes modems to go offline, and configuration loss.</p> <p>This issue occurs when the behavior of the cr10k card [slot/subslot] OIR-compatibility command is converted from default disabled to default enabled for all cable line cards.</p> <p>Workaround: Prior to exchanging line cards, configure OIR-compatibility for all slots.</p> <p>If the line card exchange occurs without configuring OIR-compatibility, and the problem has been discovered BEFORE a <b>wr mem</b> command is issued, perform the following procedure:</p> <ol style="list-style-type: none"> <li>1. Copy sec-nvram:startup-config to external box.</li> <li>2. Edit card types from MC520s-d to MC520u-d.</li> <li>3. Copy the modified file to nvram:startup-config, and also sec-nvram:startup-config</li> <li>4. Reload.</li> </ol> <p>This procedure is the only procedure which ensures that your frequency stacking and virtual interface configurations are preserved. Attempts to paste pieces of the previously stored running configuration will fail if frequency stacking or virtual interfaces are configured as the connectors must be un-assigned first.</p> <p>If a <b>wr-mem</b> has occurred, then the shutdown state, and blank configuration file for all interfaces will be written to both the primary and secondary nvram: as a result, the technique above will not work without resorting to an externally stored backup configuration for the system.</p>
CSCek31526	<p>The Inter-Process Communication (IPC) between cable line cards (CLCs) occasionally fails.</p> <p>Workaround: Reload the image to fix this issue.</p>
CSCek35970	<p>The IP ToS/DSCP byte is not overwritten for PacketCable CALEA replicated packets with the value received by GATE-SET COPS messages.</p> <p>There are no known workarounds.</p>
CSCek38537	<p>When a cable modem is moved to another channel using an upstream channel change (UCC) (init tech 1), the modem is incorrectly marked as cloned modem.</p> <p>There is no known workarounds.</p>
CSCek38598	<p>No corresponding parallel express forwarding (PXF) queue is created for the new dynamic service flow when testing the dynamic service messaging (DSX) with the <b>test cable DSA</b> command.</p> <p>The real Media Terminal Adapters (MTAs) are able to make call with DSX without any problem.</p> <p>There are no known workarounds.</p>
CSCek39428	<p>DC Directory (DCD) messages do not get captured if the <i>mac-address</i> parameter is specified in the <b>cable monitor</b> command.</p> <p>There are no known workarounds.</p>

**Table 73**      **Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCek39658	<p>The value of CMTipAddress in the IP Detail Record (IPDR) information, sent by the cable modem termination system (CMTS) when cable billing is configured is currently set to the lowest IP address numerical value on the CMTS. This value is not guaranteed to be consistent for a given CMTS.</p> <p>There are no known workarounds.</p>
CSCek41629	<p>A problem can occur on a Cisco10012 router (PRE1) running Cisco IOS Release 12.3(9a)BC7 where the cable modem termination system (CMTS) stalls for a period of time and then bursts traffic outbound from the Gigabit Ethernet interface. This causes drops on the upstream router's Gigabit Ethernet interface.</p> <p>Workaround: Perform a Performance Routing Engine (PRE) failover, or reload the CMTS.</p>
CSCek42764	<p>After an LC switchover, the Working standby interface configuration is displayed in the <b>show dsgr tunnel</b> command output.</p> <p>Workaround: Skip the standby interface when scanning cable interfaces to display the DOCSIS Set-Top Gateway (DSG) tunnel information.</p>
CSCek44348	<p>Executing the <b>show cable modem summary total</b> and <b>show controllers</b> commands creates traceback at the cable modem termination system (CMTS) console.</p> <p>There are no known workarounds.</p>
CSCin92949	<p>When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.</p> <p>This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.</p> <p>Workaround: All filter-groups specified in the CM-registration files <b>MUST</b> exist on the CMTS.</p>
CSCin98031	<p>N+1 synchronization does not occur when switching over from the Working card to the Protect card.</p> <p>There are no known workarounds.</p>
CSCsb21856	<p>Spectrum-groups with discrete frequency entries are not supported on cable line cards containing Advanced Spectrum Management functionality.</p> <p>A warning message should be generated if a spectrum-group is applied to an Advanced Spectrum Management capable upstream port.</p> <p>There are no known workarounds.</p>

**Table 73**      **Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

DDTS ID Number	Description
CSCsb29361	<p>In some circumstances, a cable modem with a downstream minimum reserved rate is allowed to register on a Cisco uBR10000 series cable modem termination system (CMTS). However, committed information rate (CIR) resources for the modem are not available. Error messages similar to the following are displayed in the unit's log:</p> <pre data-bbox="613 489 1523 590">%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow 236, CM 0004.9e95.f2a9</pre> <p>The modem is not able to receive any downstream data.</p> <p>The issue occurs only when the total reserved downstream bandwidth approaches the total available downstream bandwidth.</p> <p>There are no known workarounds.</p>
CSCsb29718	<p>The customer premises equipment (CPE) does not complete the Dynamic Host Configuration Protocol (DHCP) when moved from behind one cable modem to another.</p> <p>The following event is logged:</p> <pre data-bbox="613 915 1523 1041">...start... Jun 30 13:48:54.962: %UBR10000-3-SPOOFEDMAC: Investigating MAC=0011.2f32.c220 Cable6/1/0 sid 2900: Original MAC on sid 2899 Cable6/1/0 ...end...</pre> <p>Workaround: Enter the <b>clear cable modem</b> or <b>clear cable host</b> command.</p>

Table 73 Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)

DDTS ID Number	Description
CSCsb86099	<p>While performing a switchover, the following error message occurs. After multiple switchovers, the router unexpectedly crashes:</p> <pre>Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC2 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC3 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC4 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US2 Physical Port Link Down</pre> <p>This issue occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>• Performing a Route Processor Redundancy (RPR) switchover using the CLI.</li> <li>• Performing multiple switchovers</li> </ul> <p>There are no known workarounds.</p>
CSCsc12507	<p>When PacketCable event messaging is enabled, the cable modem termination system (CMTS) always uses the global routing table to find the route for the dynamically learned record keeping server (RKS) address. As a result, if the RKS IP address is part of a VPN routing/ forwarding (VRF) route table, CMTS fails to do the correct routing for the Remote Authentication Dial-In User Service (RADIUS) accounting messages.</p> <p>This issue occurs on a Cisco uBR10012 CMTS with a Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) based setup.</p> <p>Workaround: Perform a controlled route distribution between the VRF routing table and the global routing table so that the route for RKS server will be available on the global IPV4 routing table.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 cannot come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC02 and all Cisco IOS 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>

**Table 73**      **Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

DDTS ID Number	Description
CSCsc30294	<p>The following traceback occurs when testing line card failover while making a call from a Cisco uBR10000 series router.</p> <pre>Remote CMTS calls in progress CLI switchover working to protect. SLOT 5/0: Oct 25 17:25:20.871: %SCHED-3-STUCKMTMR: Sleep with expired managed timer 62B2ABD4, time 0xE06B58 (00:00:00 ago). -Process= "Dynamic Services Timer Process", ipl= 4, pid= 40 -Traceback= 601306F0 60130B48 60283108</pre> <p>There are no known workarounds.</p>
CSCsc32241	<p>A single tunnel interface, in a configuration of more the 1000 tunnels, does not receive the multicast traffic that it should be receiving.</p> <p>This issue occurs only in configurations with more than 1000 tunnel interfaces.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the <b>show interface</b> output are 10% of the actual packet and bit rates.</p> <p>This issue seems to occur only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsc35150	<p>If the <b>global hccp config</b> command is re-entered, the specified line card will failover.</p> <p>This issue occurs when you re-enter the <b>global hccp config</b> command and enter <b>Ctrl-Z</b> to exit. This action invokes an enter and exit at the same time and forces a line card failover.</p> <p>Workaround: To parse out the <b>config</b> command, delete the <b>config</b> command before you invoke <b>Ctrl-Z</b> or type <b>exit/end</b>. You can use <b>Ctrl-C</b> also. Either way, don't re-enter a <b>config</b> command that is already entered.</p>
CSCsc38875	<p>When a downstream cable interface on a Cisco uBR series router cable modem termination system (CMTS) experiences sustained congestion, and a significant portion of the downstream traffic is multicast traffic, Internet Group Management Protocol Version 2 (IGMPv2) Query messages might not be transmitted successfully in the downstream direction on that cable interface.</p> <p>The issue occurs when large volumes of multicast traffic, using groups that are not specified, use the cable interface <b>cable match address</b> command.</p> <p>Workaround: Ensure that all multicast traffic passing through the CMTS is classified with an appropriate <b>cable match address</b> command. This workaround may be effective only on Cisco uBR10000 series routers.</p>
CSCsc46142	<p>Modems drop offline after a line card failover.</p> <p>There are no known workarounds.</p>
CSCsc52024	<p>Interface throughput can be reduced when an output service policy is removed.</p> <p>This issue occurs if the service policy being removed defines a bandwidth percentage on the class-default.</p> <p>There are no known workarounds.</p>

Table 73 Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)

DDTS ID Number	Description
CSCsc58767	<p>Under some circumstances on a Cisco uBR10000 series cable modem termination system (CMTS), customer premises equipment (CPE) sourced multicast traffic may not be forwarded by the CMTS to other interfaces for a brief period of time.</p> <p>To diagnose this issue, look for the temporary lack of an (S,G) entry corresponding to the CPE and multicast IP addresses in the output of the <b>show ip mroute</b> command.</p> <p>The issue occurs if the CPE is transmitting to a multicast group and then stops long enough for the expiration timer of the S,G entry in the multicast routing table to time out, but not long enough for the corresponding *,G entry to time out.</p> <p>If the CPE resumes transmission to the multicast group before the *,G entry expires, then the CMTS will not allow an S,G entry to be reinstated until the *,G entry times out.</p> <p>There are no known workarounds.</p>
CSCsc61433	<p>When multiple customer premises equipment (CPE) on a bundle subinterface generate multicast traffic to the same multicast group on a Cisco uBR10000 series cable modem termination system (CMTS), the CMTS will only add one of the streams to the multicast routing table as indicated by the <b>show ip mroute</b> command.</p> <p>There are no known workarounds.</p>
CSCsc71939	<p>After a Performance Routing Engine (PRE) switchover followed by a line card (LC) switchover, if the Protect LC is reset or unexpectedly reloads, the standby PRE may crash due to a state inconsistency.</p> <p>There are no known workarounds.</p>
CSCsc73546	<p>PacketCable gates are lost during downstream (DS) load-balancing/Dynamic Channel Change (DCC).</p> <p>There are no known workarounds.</p>
CSCsc78164	<p>After performing a Performance Routing Engine (PRE) switchover, a line card may not respond to Inter-Process Communication (IPC) messages.</p> <p>This error condition occurs after PRE switchover and appears in the router log as an error such as the example shown below:</p> <pre>Dec 12 02:13:27.662: %IPCOIR-2-CARD_UP_DOWN: Card in slot 4/0 is down. Notifying lgigetherne-1 driver. Dec 12 02:13:27.662: %UBR10K_ALARM-6-INFO: ASSERT CRITICAL slot 4/0/0 Card Stopped Responding OIR Alarm - subslot 0 Dec 12 02:13:27.662: %IPCGRP-3-CMDOP: IPC command 2 (slot4/0): linecard ipc is disabled - blocking ipc command failed - Traceback= 606D0478 606D0ED4 606D1BD4 60957264 600A5E58 606D1E98 606D4B3C Dec 12 02:13:27.662: %UBR10K_ALARM-6-INFO: CLEAR CRITICAL slot 4/0/0 Card Stopped Responding OIR Alarm - subslot 0</pre> <p>Workaround: There is no workaround to avoid this problem, but if this condition occurs, the LC that is not responding to IPC messages might need to be reloaded.</p>

**Table 73**      **Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsc81321	<p>The <b>vendor</b> option is missing from the <b>show cable modem</b> command. When specifying an interface, such as <b>show cable modem c4/0 vendor</b>, the <b>vendor</b> option does not work.</p> <p>Workaround: Use a command without a specific interface to get all interfaces, such as the <b>show cable modem vendor</b> command.</p>
CSCsc82827	<p>When PacketCable Multimedia (PCMM) calls are load-balanced across the Mac-Domain using Dynamic Channel Change (DCC), loss of PCMM calls and PCMM gates occurs.</p> <p>There are no known workarounds.</p>
CSCsc91717	<p>There is a discrepancy in packet classification between the Fast Ethernet and Gigabit Ethernet interfaces.</p> <p>There are no known workarounds.</p>
CSCsc99211	<p>After switchover, some modems go offline and some calls are dropped.</p> <p>This issue occurs after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCsc99862	<p>CALEA fails if the active line card is powered down. The wiretap transfers to the standby line card.</p> <p>If a wiretap is in process and voice stream data is flowing to the DF, powering down the active line card can cause the wiretap to quit sending voice data.</p> <p>There are no known workarounds. For N+1 switchover in a wiretap, don't use the <b>power down</b> command.</p>
CSCsd03740	<p>The <b>cable upstream 0 scheduling type ?</b> command is not synchronized during N+1 switchover.</p> <p>There are no known workarounds.</p>
CSCsd13114	<p>Traceback occurs on the cable modem termination system (CMTS) console during a Hot Standby Connection-to-Connection Protocol (HCCP) switchover when the Simple Network Management Protocol (SNMP) and show commands are running.</p> <p>There are no known workarounds.</p>
CSCsd14355	<p>The Simple Network Management Protocol (SNMP)-created quality of service (QoS) profile is not available after a Performance Routing Engine (PRE) switchover; the command- created QoS profile is available after switchover.</p> <p>There are no known workarounds.</p>
CSCsd20606	<p>A parallel express forwarding (PXF) restart disables multicast traffic that matches the Multicast Quality of Service (MQoS) configuration.</p> <p>This issue occurs when an MQoS configuration is applied to cable interfaces, and PXF is restarted</p> <p>There are no known workarounds.</p>

**Table 73**      **Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

DDTS ID Number	Description
CSCsd20683	<p>A command switchover with a virtual interface (VI) configuration is not switching the whole line card.</p> <p>By default, when VI is enabled on an interface, the Hot Standby Connection-to-Connection Protocol (HCCP) line card should switchover the whole line card instead of switching an individual domain.</p> <p>There are no known workarounds.</p>
CSCsd27514	<p>Traffic on service flows with a non-zero Traffic Priority value are treated as zero priority.</p> <p>This issue occurs if there is a restart of parallel express forwarding (PXF) while the non-zero priority service flows are present.</p> <p>Workaround: Reset the affected modem.</p>
CSCsd28190	<p>PacketCable calls with upstream (US) Low Latency Queueing (LLQ) are dropped after switching over from the Protect card to the Working card.</p> <p>There are no known workarounds.</p>
CSCsd29450	<p>A Protect LC crashes after a sequence of route processor (RP) and LC switchovers.</p> <p>This issue occurs when performing a sequence of LC and Performance Routing Engine (PRE) switchovers.</p> <p>There are no known workarounds.</p>
CSCsd30267	<p>The Authentication, Authorization, and Accounting (AAA) per user process is holding memory, and the router is running out of memory.</p> <p>This issue occurs when PPP over Ethernet (PPPoE) dialing and dynamic access control lists (ACLs) are present.</p> <p>There is no known workaround.</p>
CSCsd31970	<p>On a Cisco uBR10000 series router cable modem termination system (CMTS) with redundant Performance Routing Engine (PRE) modules, new interface mode configuration commands entered on the active PRE may not be properly synchronized to the standby PRE if the <b>do show running-configuration</b> command is entered in interface configuration mode.</p> <p>This issue can lead to a configuration mismatch between the two PRE modules and can cause difficulty on PRE switchover.</p> <p>Workaround: Refrain from issuing the <b>do show running-configuration</b> command in interface configuration mode, or completely exit interface configuration mode after issuing the command.</p>
CSCsd33394	<p>On Cisco uBR10000 series routers, cable modem termination system (CMTS) upstream subscriber traffic management filters do not filter packets with a multicast destination IP address.</p> <p>Workaround: Configure and apply an IP access-list to the cable or bundle interface that applies to traffic for all the modems and customer premises equipment (CPE) on the interface.</p>

**Table 73**      **Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

DDTS ID Number	Description
CSCsd36652	<p>When configuring line card redundancy by using the <b>global HA</b> commands, duplicate RF-switch slot numbers were configured. This configuration is not allowed.</p> <p>There are no known workarounds.</p>
CSCsd43741	<p>VID data in the entPhysicalHardwareRev MIB displays the wrong value if the data field in EEPROM is missing.</p> <p>This issue affects the Entity MIB in all Cisco uBR10000 software releases, if the VID data field is not programmed.</p> <p>There are no known workarounds.</p>
CSCsd44373	<p>Certain upstream (US) parameters are not copied from a Working cable line card (CLC) to the Protect CLC during a failover under the following conditions: -upstream docsis mode, -upstream modulation profile, -upstream data-backoff.</p> <p>Because the original settings on the Protect CLC remain, it is possible after a failover to have a Data-over-Cable Service Interface Specification (DOCSIS) mode and modulation profile inconsistent with that of the Working CLC prior to the failover. This inconsistency can create problems. For example, if a Time Division Multiple Access (TDMA)-only Working CLC fails over to a Protect CLC configured with Asynchronous Time Division Multiple Access (ATDMA), the cable modems will switch to ATDMA mode. When the Protect fails back to the TDMA-only Working CLC, the cable modems will continue to use ATDMA and lose IP connectivity.</p> <p>There are no known workarounds.</p>
CSCsd47667	<p>The cable meter feature is causing redundancy to fail between PRE2's due to Inter-Process Communication (IPC) timeouts.</p> <p>This issue occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC2 or 12.3(17a)BC.</p> <p>Workaround: Reload the standby PRE2.</p>
CSCsd57064	<p>When using an IP Protocol field value of 1, the Data-over-Cable Service Interface Specification (DOCSIS) 1.1 classifier might match other or all IP traffic to this classifier instead of just Internet Control Message Protocol (ICMP) traffic (IP Protocol 1 as per RFC1700).</p> <p>This issue can occur on a Cisco cable modem termination system (CMTS) running Cisco IOS Release 12.3(13a)BC1.</p> <p>There are no known workarounds.</p>
CSCsd58566	<p>Multicast quality of service (QoS) counters can drop packets across different switchovers.</p> <p>There are no known workarounds.</p>

**Table 73**      **Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsd58686	<p>If configured through the DOCS-DSG-IF-MIB, the DOCSIS Set-Top Gateway (DSG) configuration gets lost after the Performance Routing Engine (PRE) switchover.</p> <p>This issue occurs because the Simple Network Management Protocol (SNMP) configuration is not preserved between PRE switchover in Cisco IOS Release 12.3BC.</p> <p>There are no known workarounds.</p>
CSCsd59817	<p>On the MC520u card, signal-to-noise ratio (SNR) values may drop on a upstream, which can cause modems to drop offline.</p> <p>This issue occurs on Cisco uBR10000 series routers running Cisco IOS Release 12.3(9a)BC8 with multiple MC520u cards.</p> <p>Workaround: Either disable/enable pre-equalization on the upstream, or change the modulation on the upstream.</p>
CSCsd65022	<p>The downstream (DS) bandwidth scheduler doesn't work correctly after a PacketCable Multimedia (PCMM) call switchover.</p> <p>There are no known workarounds except to reload the cable modem termination system (CMTS).</p>
CSCsd67236	<p>A policy-based routing (PBR) map with a set clause does not act on matching packets.</p> <p>This issue occurs on PRE1s on Cisco uBR10000 series routers only.</p> <p>There are no known workarounds.</p>
CSCsd77494	<p>After several iterations of PacketCable (PC) and PacketCable Multimedia (PCMM) calls, downstream (DS) does not work correctly.</p> <p>There are no known workarounds. A cable modem termination system (CMTS) reload is required to recover.</p>
CSCsd77991	<p>A line card on the Cisco uBR10000 series router unexpectedly crashes.</p> <p>This issue occurs when the <b>clear cable modem</b> command is executed for a multicast address.</p> <p>Workaround: Do not use the <b>clear cable modem</b> command for multicast addresses.</p>
CSCsd78370	<p>The privacy bit value of the Multicast entries present on the cable modem termination system (CMTS) host database change after an Route Processor Redundancy (RPR) Switchover.</p> <p>This issue occurs when adding multicast entries into the CMTS host database, but before the RPR Switchover.</p> <p>There are no known workarounds.</p>
CSCsd83029	<p>The Media Terminal Adapters (MTA) goes offline and stays offline after 24 hours of bulk calls.</p> <p>There are no known workarounds.</p>

**Table 73 Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

DDTS ID Number	Description
CSCsd95113	<p>A cable modem, when enforced with a quality of service (QoS) profile created using the cdxCmtsCmQosProfile MIB, accepts the profile and <b>show cable modem reg</b> shows the modem with the enforced profile. However, the same cable modem, after reset, does not come online with the enforced profile. Instead, it comes online with the default profile. In contrast, the same modem (when enforced with the QoS profile created using the CLI) comes online after reset with the enforced profile, not the default profile.</p> <p>This behavior is irrespective of platforms and whether the QoS profile is created using the CLI or the Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCsd95828	<p>Telnet or Secure Shell (SSH) access to the Cisco uBR10000 series router fails after a Performance Routing Engine (PRE) switchover/Failover.</p> <p>This issue occurs on Cisco uBR10000 series routers running Cisco IOS Release 12.3(13a)BC3 with a line vty configured for "login local" on the active PRE.</p> <p>Workarounds: Either configure a password under the line vty, or configure Authentication, Authorization, and Accounting (AAA) authentication as follows:</p> <pre>Router#conf term Enter the following configuration commands, one per line. End with CNTL/Z.  Router(config)#aaa new-model Router(config)#aaa authentication login ABC local Router(config)# Router(config)#line vty 0 4 Router(config-line)#login authentication ABC</pre>
CSCsd96270	<p>Parallel express forwarding (PXF) crash info files are missing a portion of the PXF direct memory access (DMA) information.</p> <p>This issue occurs after a restart of PXF; if a crashinfo file is requested, the file is missing this information.</p> <p>There are no known workarounds.</p>
CSCsd97968	<p>Support for additional error checking was added to the code.</p>
CSCse00902	<p>Various <b>show</b> commands use improper case and spelling.</p> <p>There are no known workarounds.</p>
CSCse02543	<p>When some modems are in the reject state and a <b>clear cable modem reject delete</b> command is issued, a CM_INCONSISTENCY message is generated.</p> <p>Workaround: Do not use the <b>clear cable modem reject delete</b> command.</p>
CSCse02868	<p>A spurious memory access error occurred involving if-cons to cable line card slots and a Performance Routing Engine (PRE) failover.</p> <p>There are no known workarounds.</p>
CSCse05422	<p>A router crashes with the following error message:</p> <p>PXF DMA Error - End of Descriptor Before Cmd Byte Length</p> <p>There are no known workarounds.</p>

Table 73 Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)

DDTS ID Number	Description
CSCse05641	<p>Syslog messages with new lines get truncated on the syslog server and are treated as invalid.</p> <p>This issue occurs because the system event message has message-text with a new line (\n), causing the message to be in two lines rather than a single line.</p> <p>As a result, the message appears in the cable modem termination system (CMTS) logs in separate lines:</p> <pre>Apr 17 15:01:22.489 EDT: %UBR10000-3-MACADDRERR: DHCP Msg with non unicast MAC address. Master Interface Cable7/0/0 Input Interface SID = 65535 MAC = 0000.0000.0000</pre> <p>Ideally, the message should be in one line:</p> <pre>Apr 17 15:01:22.489 EDT: %UBR10000-3-MACADDRERR: DHCP Msg with non unicast MAC address. Master Interface Cable7/0/0 Input Interface SID = 65535 MAC = 0000.0000.0000</pre> <p>There are no known workarounds.</p>
CSCse08883	<p>After two Performance Routing Engine (PRE) switchovers, a non-functioning High Availability (HA) LC becomes active on the PROTECTA MC520H line card.</p> <p>There are no known workarounds.</p>
CSCse16505	<p>The <b>test cable metering abort</b> command doesn't abort the metering if the streaming export is connect failed.</p> <p>There are no known workarounds.</p>
CSCse21591	<p>If you configure Dynamic Upstream Load Balancing on several upstreams (in the same MAC Domain and in the same load balancing (LB) Group) for the first time before executing a <b>no cable upstream x shut</b> command on those upstreams, only one member of the group will have working Dynamic LB. The other upstreams will have DLB stuck in the "initial" state.</p> <p>This issue occurs on Cisco uBR10000 series routers running Cisco IOS Release 12.3(9a)BC9.</p> <p>Workaround: Either use Static LB or enter the <b>no cable upstream x shutdown</b> command at the upstream (US) Interfaces you want to have DLB configured on, and then enter the DLB configurations for the first time.</p> <p>Further Problem Description: This issue was not encountered if DLB was configured after the US interfaces were unshut. This problem only occurs if you configure DLB first, and then unshut the US interfaces.</p>

**Table 73 Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

DDTS ID Number	Description
CSCse22063	<p>On a Cisco uBR10000 series router running the cable modem termination system (CMTS), a manual Hot Standby Connection-to-Connection (HCCP) N+1 line card switchover can fail if one cable interface on the line card being switched over is shutdown. An error message appears, such as:</p> <pre data-bbox="613 457 1218 489">% HCCP 2 60: aborts switchover. Request later.</pre> <p>This issue occurs when the individual cable interface was in the shutdown state when CMTS was activated. The problem does not tend to occur if the cable interface was shutdown after CMTS has been operational. A manual N+1 line card switchover may be initiated with the command: <b>redundancy linecard-group switchover from slot/subslot</b></p> <p>Workaround: Activate shutdown cable interface with the cable interface <b>no shutdown</b> command. Optionally, add the cable interface <b>no keepalive</b> command if no cable modems are expected to be online on the interface.</p>
CSCse22482	<p>After a Performance Routing Engine (PRE) failover, downstream voice traffic moves from dynamic flow to primary flow.</p> <p>There are no known workarounds.</p>
CSCse24179	<p>The dynamic service flow created for PacketCable Multimedia (PCMM) sessions for the Speed Preview application hang.</p> <p>Workaround: Because the Speed Preview application cannot set the PCMM T3 timer (DOCSIS T8 timer), the only way to clean up the service flow is to identify the flows that are stuck and enter <b>test cable dsd ip-addr-of-modem</b> command.</p>
CSCse24904	<p>When a lockout of the Working card is followed by online insertion and removal (OIR), the following two problems occur: 1) OIR switches from the Working card to the Protect card, dropping all the cable modems. 2) After the Working card is back from the OIR, traffic stays on the Protect card with the cable modems down, and the Working card has lockout active. Clearing lockout fails, and because the Working card is standby, reverting to the Working card would also fail.</p> <p>There are no known workarounds.</p>
CSCse25429	<p>While netbooting the cable modem termination system (CMTS) with the latest geo_cable image, the CMTS crashes.</p> <p>This issue occurs when CMTS has unsupported DOCSIS Set-Top Gateway (DSG)1.2 configurations on the startup at the time of netbooting.</p> <p>Workaround: Load the image without having any unsupported DSG configurations on the startup.</p>
CSCse27060	<p>ifTable objects are not created after online insertion and removal (OIR) of the 5x20 card.</p> <p>Workaround: Reboot the cable modem termination system (CMTS) after the card swap.</p>
CSCse27391	<p>The Hot Standby Connection-to-Connection Protocol (HCCP) stops working properly if a switchover is required from the Working card to the Protect card.</p> <p>No errors are shown. Switching back to the Working card gets the cable modems back online.</p> <p>Workaround: Reload the box; a reload/reseat of the line cards does not work.</p>

Table 73 Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)

DDTS ID Number	Description
CSCse28069	High CPU usage in the TTY background occurs on a terminal server connected to a Cisco uBR10000 series router (PRE2) when the <b>modem inout</b> command is configured.  Workaround: Disable the <b>modem inout</b> command.
CSCse32310	An MC520 crash occurs.  There are no known workarounds.
CSCse32901	Overlapping RF switch slots numbers are configured in a global High Availability (HA) 4+1 setup.  There are no known workarounds.
CSCse35261	When a Cisco uBR10000 series router with an MC-520S-D line card is being used to carry Circuit Emulation over IP (CEoIP) traffic over an Unsolicited Grant Services (UG) service flow, the traffic experiences an occasional packet loss upstream direction and excessive jitter in both the upstream and downstream directions.  Workaround: Use the Cisco uBR7246VXR with the uBR28U line card and Cisco IOS Release 12.3(13a)BC4 image for the CEoIP application.
CSCse39194	Unencrypted traffic, such as broadcast Address Resolution Protocol (ARP) requests, can leak into an Layer 2 (L2) virtual private network (VPN) supported by a Cisco cable modem termination system (CMTS).  There are no known workarounds.
CSCse42277	Configuring a new High Availability (HA) Working line card on the cable modem termination system (CMTS) crashes the standby Performance Routing Engine (PRE) if the RF switch name cannot be resolved to the Domain Name System (DNS).  Workaround: Verify that the RF switch name can be resolved to DNS before adding Working line cards.
CSCse44033	The cable modem termination system (CMTS) allows more than 8 multicast addresses per Multicast service ID (SID) per modem and also forwards traffic on all the multicast addresses per multicast SID per modem.
CSCse44203	The <b>show cable leasequery-filter interface requests-filtered</b> command is not updated when the upstream threshold=0.  There are no known workarounds.
CSCse45342	Configuring cable default-tos-qos10 tos-overwrite and resetting the modem does not create a new qos-profile. The modem comes online with the existing profile.  The problem occurs on modems provisioned in Data-over-Cable Service Interface Specification (DOCSIS) 1.0 mode when the default tos-mask and tos-value are configured.  There are no known workarounds.
CSCse48188	After a Performance Routing Engine (PRE failover), the dynamic service flow to Multiprotocol Label Switching (MPLS) virtual private network (VPN) feature no longer works.  There are no known workarounds.

**Table 73** *Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCse48454	Entering a <b>shut/no shut</b> command on an interface triggers infinite switchovers. There are no known workarounds.
CSCse49677	The Working card and its upstream (US) Protected line card are stuck in a non-functional state during a Hot Standby Connection-to-Connection Protocol (HCCP) switchover. There are no known workarounds.
CSCse50424	On a Cisco uBR10000 series router, PRE2 is experiencing high CPU usage and crashes when querying the customer premises equipment (CPE) (40 CPEs) by the Simple Network Management Protocol (SNMP). There are no known workarounds.
CSCse50735	After a cable line card failover, the dynamic Service Flow (SF)-to-Multiprotocol Label Switching (MPLS) virtual private network (VPN) mapping feature no longer works. There are no known workarounds.
CSCse52836	On a Cisco uBR10000 series cable modem termination system (CMTS), the first cable modem online in a modem created Data-over-Cable Service Interface Specifications (DOCSIS) 1.0 QoS profile may not have its ToS byte correctly overwritten when the <b>cable default-tos-qos10 tos-overwrite</b> command is implemented. There are no known workarounds.
CSCse54378	On a Cisco uBR10000 series router running Cisco IOS image ubr10k-k9p6u2-mz.2006-06-02.123_17_BC, tracebacks are found at sch_rp_download_debug_info when you attempt to configure an already assigned address. There are no known workarounds.
CSCse55592	Two typos exist in the microcode under the Cisco uBR10000 PRE2 platform that can potentially result in some feature errors (including Input/Output ACL, MLP Rx, MLP Tx, MAC Rewrite, and WRED Calc.) There are no known workarounds.
CSCse55595	After unconfiguring global High Availability (HA) commands and then issuing a Performance Routing Engine (PRE) failover, certain global HA commands are still configured on the new active PRE.  This issue occurs after issuing a <b>do show run   beg redundancy</b> command followed by a <b>Ctrl-C</b> when in configuration mode, which causes the standby PRE not to recognize the commands to un-configure global HA.  Workaround: While un-configuring global HA do not issue a <b>do show run   beg redundancy</b> command followed by a <b>Ctrl-C</b> .

Table 73 Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)

DDTS ID Number	Description
CSCse55926	<p>Modems get stuck in init(o) when upgrading from Cisco IOS Release 12.3(9a)BC9 to 12.3(17a)BC1.</p> <p>When you first upgrade, and the configuration is upgraded from the Cisco IOS Release 12.3 (9a)BC9 to Cisco IOS Release 12.3 (17a)BC1 configuration, all modems get stuck in init(o). They remain stuck in init(o) until you either enter the <b>write memory</b> command and reload the box, or you reload the active Parallel Express Forwarding (PXF).</p> <p>Workaround: Enter the <b>write memory</b> command after upgrading and then reload the router, or reload the PXF.</p>
CSCse57637	<p>The Low Latency Queueing (LLQ) upstream scheduler option does not distinguish between Non Real Time Polling Service (nrtPS) and Real Time Polling Service (rtPS) flows correctly.</p> <p>There are no known workarounds.</p>
CSCse58398	<p>On a Cisco uBR10000 platform running Cisco IOS Release 12.3(17a)BC1, when you erase the start up configuration file, copy a fresh configuration file to the start up, and reload the router, most of the cable-related configurations and generic configurations (including IP address) under the cable interface disappear. Only when you copy the start-up to run-config do the configurations appear again.</p> <p>There are no known workarounds.</p>
CSCse58522	<p>Random modems in online (pt) are not pingable.</p> <p>This problem occurs on Cisco uBR10012 systems running on Cisco IOS Release 12.3(9a)BC9 and Cisco IOS Release 12.3(13a)BC2. The problem occurs on CMTS systems configured with frequency stacking and virtual interfaces.</p> <p>There are no known workarounds.</p>
CSCse60284	<p>Embedded Media Terminal Adapters (eMTAs) are not properly reported by the variable "docsIfCmtsCmStatusUpChannellfIndex".</p> <p>Workaround: Reload the box, or issue the <b>cable upstream max-port 5</b> command.</p>
CSCse61799	<p>The cable modem termination system (CMTS) drops 10 packets to the Mediation server during Revertback N+1 Switchover (during Protect to Working). No packet drop to Mediation server occurs during the N+1 Switchover from Working to Protect.</p> <p>There are no known workarounds.</p>
CSCse62054	<p>The error message "Removing host database entry for modem and traceback" occurs on the cable modem termination system (CMTS) in syslog.</p> <p>There are no known workarounds.</p>
CSCse63548	<p>When the logging console is enabled and the <b>show hccp brief</b> command is issued, tracebacks are found in the secondary Performance Routing Engine (PRE).</p> <p>There are no known workarounds.</p>
CSCse64138	<p>When load-balancing is used, some modems might go into init(rc) after an upstream channel change (UCC).</p> <p>There are no known workarounds.</p>

**Table 73**      **Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCse66329	<p>The router may reload unexpectedly upon execution of the <b>show pxf cpu qos</b> command with a non-cable interface specified.</p> <p>Workaround: If this command must be executed, ensure that a cable interface is specified.</p>
CSCse67808	<p>The cdpCacheTable contains entries with index 4294967295 that are only available using the Simple Network Management Protocol (SNMP) <b>get-next</b> command. When the <b>get-one</b> command is used to retrieve the same value, a <code>NO_SUCH_INSTANCE_EXCEPTION</code> is returned.</p> <p>This issue appears to be related to the management ethernet port on the secondary Performance Routing Engine (PRE) in a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCse68483	<p>Unusual characters (parser issue) are generated on the terminal output (console or Telnet session).</p> <p>This issue only occurs when the cable modem termination system (CMTS) is configured with baseline privacy interface (BPI) and the <b>debug cable privacy</b> command is enabled on a non-Cisco cable modem.</p> <p>Workaround: Turn off the debug, disconnect the session, and re-connect.</p>
CSCse69638	<p>Modems go offline after N+1 switch over with Spectrum configurations.</p> <p>There are no known workarounds.</p>
CSCse71725	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>cable monitor</b> command does not successfully monitor upstream bandwidth request messages.</p> <p>There are no known workarounds.</p>
CSCse81859	<p>On a Cisco uBR10012 router running on Cisco IOS Release 12.3(13a)BC2, the Cisco uBR10-MC5X20U line card crashed with the following error:</p> <p>Cause 80000010 (Code 0x4): Address Error (load or instruction fetch) exception Crash info file was written and the LC was reloaded</p> <p>There are no known workarounds.</p>
CSCse77306	<p>You cannot get Simple Network Management Protocol (SNMP) MIB information after a Hot Standby Connection-to-Connection Protocol (HCCP) and Performance Routing Engine (PRE) switchover.</p> <p>Workaround: Issue the <b>cable upstream max-ports x</b> command under the affected cable interfaces, or reload PRE</p>

**Table 73** Open Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)

DDTS ID Number	Description
CSCse77897	Simple Network Management Protocol (SNMP) polling of the cable modems reports the modems on wrong interfaces. The <b>show</b> command output on the cable modem termination system (CMTS) shows the right information.  This issue occurs on Cisco IOS Release 12.3(9a) BC7 on PRE1 and PRE2.  There are no known workarounds.
CSCse78143	On a Cisco uBR10000 series cable modem termination system (CMTS), the <b>show cr10k-rp cable x/y/z sid</b> command does not allow the service identifier (SID) value to be set to values greater than 8176. As a result, queues associated with downstream multicast quality of service (QoS) SIDs cannot be examined.  There are no known workarounds.

## Resolved Caveats for Release 12.3(17a)BC2

Table 74 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17a)BC2.

**Table 74** Resolved Caveats for Cisco IOS Release 12.3(17a)BC2

DDTS ID Number	Description
CSCek34311	The Performance Routing Engine (PRE) unexpectedly reloads if the <b>cable upstream n frequency up-freq-hz</b> command is repeated more than 500 times.  There are no known workarounds.
CSCek37177	The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.  Cisco has made free software available to address this vulnerability for affected customers.  This issue is documented as Cisco bug ID <a href="#">CSCek37177</a> .  There are workarounds available to mitigate the effects of the vulnerability.  This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-tcp">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-tcp</a>
CSCek37518	Client information is not displayed in the <b>show cable dsd tunnel ?</b> command when the tunnel group is not associated with a downstream interface.  There are no known workarounds.
CSCek48215	With shared connector config (frequency stacking), modems do not come up online on all the interfaces.  Workaround: Reset connector config. Reset the LC.

**Table 74 Resolved Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)**

DDTS ID Number	Description
CSCsd31933	<p>If many modems are not registered at the cable modem termination system (CMTS) and logging is enabled at the CMTS console, a route processor may crash due to high CPU utilization.</p> <p>This condition occurs on a Cisco uBR10000 series router.</p> <p>Workaround: Avoid enabling the logging console message at the CMTS console if many modems are not registered.</p>
CSCsd67203	<p>The Cable Metering process stalls on a Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC2.</p> <p>This issue causes a memory leak, which eventually requires the Cable Modem Termination System (CMTS) to be reloaded when the <b>cablesflog</b> command is configured. Messages such as: “%% Low on memory; try again later” appear when accessing the box, issuing <b>show</b> commands, or configuring the CMTS.</p> <p>Workarounds: 1. Remove the <b>cable sflog</b> command. 2. Failover the Performance Routing Engine (PRE), and reload the CMTS to free memory.</p>
CSCsd90835	<p>High downstream (DS) latency occurs on the MC520.</p> <p>The primary symptoms include excessive ping times (up to 1000 milliseconds), and spurious memory access.</p> <p>There are no known workarounds.</p>
CSCse00016	<p>The PXF_Crashinfo file write operation fails to complete.</p> <p>This issue may occur due to an unscheduled restart of parallel express forwarding (PXF).</p> <p>There are no known workarounds.</p>
CSCse00861	<p>On a Cisco uBR10000 series the cable modem termination system (CMTS), cable modems and connected customer premises equipment (CPE) are not able to be pinged after a Hot Standby Connection-to-Connection Protocol (HCCP) line card failover to a Protect line card.</p> <p>This issue can affect cable modems if they are using baseline privacy interface (BPI) encryption and connected to the second upstream channel to be sharing an upstream connector using the frequency stacking functionality.</p> <p>Workaround: Disable BPI encryption and/or not use frequency stacking, or connector sharing, when HCCP switchovers may occur. Affected cable modems and CPE will become pingable again after the failed over MAC domain is reverted back from the Protect line card to the Working line card. Affected cable modems may also regain IP connectivity after being reset.</p>
CSCse22463	<p>The MC520u card in an N+1 setup is not responding with a non-default connector configuration.</p> <p>This issue occurs upstream when a JIB connected to a connector on another JIB causes the line card to hang the cable upstream connector.</p> <p>Workaround: Restore the connector config so that upstream is connected to a connector on the same JIB and reset the line card.</p>

**Table 74** Resolved Caveats for Cisco IOS Release 12.3(17a)BC2 (continued)

DDTS ID Number	Description
CSCse42638	<p>On a newly configured cable interface on a Cisco uBR10000 series router, cable modem termination system (CMTS) modems may not come online due to the interface not transmitting Upstream Channel Descriptor (UCD) messages to cable modems.</p> <p>This issue can occur on a newly configured upstream that uses spectrum-groups.</p> <p>Workaround: Issue one or more <b>shut/no shut</b> commands on the interface.</p>
CSCse80713	<p>The cable modem termination system (CMTS) reports the following error after an MC520H card is inserted:</p> <pre>SLOT 5/0: Jul 17 16:05:43.960: %UBR10000-3-I2CERR: Cable5/0/2: I2C bus is busy, cannot access slave device at interrupt level 3.</pre> <p>Although all cable modems come up online as soon as the PacketCable (PC) traffic starts, a line card (LC) switchover occurs.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(17a)BC1

Table 75 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17a)BC1.

**Table 75** Open Caveats for Cisco IOS Release 12.3(17a)BC1

DDTS ID Number	Description
CSCee39660	<p>The cable modem termination system (CMTS) reports a traceback error during a Performance Routing Engine (PRE) switchover.</p> <p>There are no known workarounds.</p>
CSCeh48889	<p>The INVALIDSIDPOSITION message occurs on an interface when a large number of cable modems are going online and offline at once</p> <p>For example:</p> <pre>%UBR10000-3-INVALIDSIDPOSITION: Invalid SID (4184) position for interface Cable5/0/0: CM 00d1.1477.7451:Is used by CM 00d0.d726.ef0b SFID 6813 SID 4184. SID container info: start 744 end 6967 -Traceback= 6030A628 6030A844 6030B098 602F81FC 603A480C 605E1398 605E137C</pre> <p>One typical trigger for this message is the <b>clear cable modem delete</b> or <b>clear cable modem oui oui delete</b> command. The affected modem is kicked offline and will usually come back online later. Many different modems may be affected.</p> <p>Workaround: <b>Shut /no shut</b> the affected cable interface, or delete most modems on the cable interface.</p> <p>Alternative workaround: Reduce the number of cable modems on the affected cable interface by moving modems to other ports.</p>

**Table 75** Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)

DDTS ID Number	Description
CSCei22859	<p>The secondary service does not pass traffic after a line card switchover.</p> <p>This issue is likely related to payload header suppression (PHS) traffic and switchovers.</p> <p>Workaround: Do not use PHS.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are being forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCei54281	<p>With N+1 switchovers, the number of expected customer premises equipment (CPE) devices does not get reflected in the <b>show cable modem verbose</b> command.</p> <p>This issue occurs in a Performance Routing Engine High Availability (HA) configuration.</p> <p>There are no known workarounds.</p>
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>
CSCei69955	<p>Unsolicited Grant Services (UGS) service flows (SFs) move to the provisioned state when the channel-width and mini-slot values are changed.</p> <p>There are no known workarounds.</p>
CSCej39802	<p>An entry for an authorized mcast group is missing in the docsBpi2CmtsIpMulticastMapTable after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCej52423	<p>The wrong number of bytes are suppressed and packet drops occur on the dial shelf controller (DSC) when adding payload header suppression (PHS) and line card (LC) switchover.</p> <p>This issue occurs when performing a switchover while using LC redundancy and Multiple PHS for a secondary service flow (SF).</p> <p>Workaround: Do not use PHS with multiple rules for an SF if you are using N+1.</p>
CSCej88404	<p>The output of the <b>show cable modem interface docsis device-class</b> shows <b>unreported</b> under the <b>device class</b> as follows when the command is issued:</p> <pre>Router#show cable modem c8/1/0 docsis device-class MAC Address      I/F          MAC              Prim  Reg  Device Class                   State        Sid   Ver   CM PS MTA STB 000f.9f1f.7220   C8/1/0/U0   online          3     1.0 &lt;Unreported&gt; 0011.ae00.51da   C8/1/0/U0   online(pt)      4     2.0 &lt;Unreported&gt; 000f.9f56.77ca   C8/1/0/U0   online          5     1.0 &lt;Unreported&gt; 0000.aaaa.bbbb   C8/1/0/U0   online          10    2.0 &lt;Unreported&gt;</pre> <p>This output is purely informational and has no operational impact on the system.</p> <p>There are no known workarounds.</p>

**Table 75**      **Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCek20675	Support is added for the <b>show pxf cable source-verify</b> command for PRE2. There are no known workarounds.
CSCek21720	Traceback occurs with packet intercept during a line card (LC) switchover in PRE2.  This issue occurs when the LC switchover is performed while PacketCable (PC) calls and class features are in progress.  There are no known workarounds
CSCek23320	Simple Network Management Protocol (SNMP)-related traceback is seen when the image is loaded with the attached cable modem termination system (CMTS) configuration:  *Dec 21 16:11:28.148: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/1, changed state to up Dec 21 16:12:08.141: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61156234 reading 0x0 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 61156234 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:12:08.141: %ALIGN-3-TRACE: -Traceback= 6115623C 6092C8DC 6092D3CC 6092D81C 6092D8AC 60DA70A0 60DA43EC 60DA42B8 Dec 21 16:14:11.138: %AAAA-3-DROPACCTSNDFAIL: Accounting record dropped, send to server failed: system-start  There are no known workarounds.
CSCek24075	Zero nodes are reported in the <b>show srp topology</b> command.  There are no known workarounds.
CSCek27678	The <b>show access-lists</b> command displays the access control lists (ACLs) for deleted packet filter groups. The corresponding internal ACLs are not removed, even after the packet filter group is deleted.  In addition, the <b>show cable filter</b> command lists the reserved ACL group 255 index 1 with drop action, even if all the cable filter configurations have been removed from the cable modem termination system (CMTS).  There are no known workarounds.

Table 75 Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)

DDTS ID Number	Description
CSCek29193	<p>Swapping unlike MC520 line cards (s, u) causes modems to go offline, and configuration loss.</p> <p>This issue occurs when the behavior of the cr10k card [slot/subslot] OIR-compatibility command is converted from default disabled to default enabled for all cable line cards.</p> <p>Workaround: Prior to exchanging line cards, configure OIR-compatibility for all slots.</p> <p>If the line card exchange occurs without configuring OIR-compatibility, and the problem has been discovered BEFORE a <b>wr mem</b> command is issued, perform the following procedure:</p> <ol style="list-style-type: none"> <li>1. Copy sec-nvram:startup-config to external box.</li> <li>2. Edit card types from MC520s-d to MC520u-d.</li> <li>3. Copy the modified file to nvram:startup-config, and also sec-nvram:startup-config</li> <li>4. Reload.</li> </ol> <p>This procedure is the only procedure which ensures that your frequency stacking and virtual interface configurations are preserved. Attempts to paste pieces of the previously stored running config will fail if frequency stacking or virtual interfaces are configured as the connectors must be un-assigned first.</p> <p>If a <b>wr-mem</b> has occurred, then the shutdown state, and blank config file for all interfaces will be written to both the primary and secondary nvram: as a result, the technique above will not work without resorting to an externally stored backup configuration for the system.</p>
CSCek31526	<p>The Inter-Process Communication (IPC) between cable line cards (CLCs) occasionally fails.</p> <p>Workaround: Reload the image to fix this issue.</p>
CSCek34311	<p>The Performance Routing Engine (PRE) unexpectedly reloads if the <b>cable upstream n frequency up-freq-hz</b> command is repeated more than 500 times.</p> <p>There are no known workarounds.</p>
CSCek35970	<p>The IP ToS/DSCP byte is not overwritten for PacketCable CALEA replicated packets with the value received by GATE-SET COPS messages.</p> <p>There are no known workarounds.</p>
CSCek38537	<p>When a cable modem is moved to another channel using an upstream channel change (UCC) (init tech 1), it is incorrectly marked as cloned modem.</p> <p>There is no known workaround.</p>
CSCek38598	<p>No corresponding parallel express forwarding (PXF) queue is created for the new dynamic service flow when testing the dynamic service messaging (DSX) with the <b>test cable DSA</b> command.</p> <p>The real Media Terminal Adapters (MTAs) are able to make calls with DSX without any problem.</p> <p>There are no known workarounds.</p>

Table 75 Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)

DDTS ID Number	Description
CSCek39428	DC Directory (DCD) messages do not get captured if the <i>mac-address</i> parameter is specified in the <b>cable monitor</b> command.  There are no known workarounds.
CSCek39605	An MC520S cable line card unexpectedly reloads in a Cisco uBR10000 series chassis.  The issue occurs while running Cisco IOS Release 12.3(9a)BC4.  There are no known workarounds.
CSCek39658	The value of CMTipAddress in the IP Detail Record (IPDR) information, sent by the cable modem termination system (CMTS) when cable billing is configured is currently set to the lowest IP address numerical value on the CMTS. This value is not guaranteed to be consistent for a given CMTS.  There are no known workarounds.
CSCek40860	A Cisco uBR10000 router running Cisco IOS Release 12.3(13a)BC2 might lose partial configuration after a Performance Routing Engine (PRE) failover. Missing configuration cannot be manually added back via CLI, parser gives an error. Entering a “?” does not show the missing commands as listed options.  This issue typically occurs after a PRE crash/failover. This issue is seen with Cisco IOS Release 12.3(13a)BC2 but not with Cisco IOS Release 12.3(9a)BCx.  Workaround: Perform a <b>wr mem</b> on active PRE and reload the standby PRE after upgrading from Cisco IOS Release 12.3(9a)BCx to 12.3(13a)BC2.
CSCin92949	When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.  This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.  Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.
CSCin98031	N+1 synchronization does not occur when switching over from the Working card to the Protect card.  There are no known workarounds.
CSCsb21856	Spectrum-groups with discrete frequency entries are not supported on cable line cards containing Advanced Spectrum Management functionality.  A warning message should be generated if such a spectrum-group is applied to an Advanced Spectrum Management capable upstream port.  There are no known workarounds.
CSCsb26657	The toaster feed_back context rate is excessive when multicast traffic is present.  There are no known workarounds.

**Table 75**      **Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)**

DDTS ID Number	Description
CSCsb29361	<p>In some circumstances, a cable modem with a downstream minimum reserved rate is allowed to register on a Cisco uBR10000 series cable modem termination system (CMTS). However, committed information rate (CIR) resources for the modem are not available. Error messages similar to the following are displayed in the unit's log:</p> <pre data-bbox="613 489 1523 594">%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow 236, CM 0004.9e95.f2a9</pre> <p>The modem is not able to receive any downstream data.</p> <p>The issue occurs only when the total reserved downstream bandwidth approaches the total available downstream bandwidth.</p> <p>There are no known workarounds.</p>
CSCsb29718	<p>The customer premises equipment (CPE) does not complete the Dynamic Host Configuration Protocol (DHCP) when moved from behind one cable modem to another.</p> <p>The following event is logged:</p> <pre data-bbox="613 919 1523 1045">...start... Jun 30 13:48:54.962: %UBR10000-3-SPOOFEDMAC: Investigating MAC=0011.2f32.c220 Cable6/1/0 sid 2900: Original MAC on sid 2899 Cable6/1/0 ...end...</pre> <p>Workaround: Enter the <b>clear cable modem</b> or <b>clear cable host</b> command.</p>

**Table 75** Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)

DDTS ID Number	Description
CSCsb86099	<p>While performing a switchover, the following error message occurs. After multiple switchovers, the router unexpectedly crashes:</p> <pre>Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC2 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC3 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC4 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US2 Physical Port Link Down</pre> <p>This issue occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>• Performing a Route Processor Redundancy (RPR) switchover using the CLI.</li> <li>• Performing multiple switchovers</li> </ul> <p>There are no known workarounds.</p>
CSCsb93608	<p>When congestion with tail drops occurs on a downstream interface, a 15% increase in CPU utilization occurs on the 2x8 cable line card.</p> <p>There are no known workarounds.</p>
CSCsc10117	<p>When a cable modem termination system (CMTS) bundle interface has 100,000 Address Resolution Protocol (ARP) entries, entering interface configuration mode at that bundle hogs the CPU for 15-20 seconds.</p> <p>This issue occurs when the bundle interface has a large number of entries in the ARP and Forwarding Information Base (FIB) tables.</p> <p>Workaround: Enter bundle interface configuration mode during a maintenance window, or split one large bundle into several smaller bundle.</p>

**Table 75 Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)**

DDTS ID Number	Description
CSCsc12507	<p>When PacketCable event messaging is enabled, the cable modem termination system (CMTS) always uses the global routing table to find the route for the dynamically learned record keeping server (RKS) address. As a result, if the RKS IP address is part of a VPN routing/ forwarding (VRF) route table, CMTS fails to do the correct routing for the Remote Authentication Dial-In User Service (RADIUS) accounting messages.</p> <p>This issue occurs on a Cisco uBR10012 CMTS with an Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) based setup.</p> <p>Workaround: Perform a controlled route distribution between the VRF routing table and the global routing table so that the route for RKS server will be available on the global IPV4 routing table.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 can not come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC02 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>
CSCsc27520	<p>When the Network Time Protocol (NTP) clock gets updated, the clock on the Performance Routing Engine (PRE) changes as expected, however, the MC520 clock does not get updated.</p> <p>Workaround: Restart the cable modem termination system (CMTS) or the line card.</p>
CSCsc30294	<p>The following traceback occurs when testing line card failover while making a call from a Cisco uBR10000 series router.</p> <pre>Remote CMTS calls in progress CLI switchover working to protect. SLOT 5/0: Oct 25 17:25:20.871: %SCHED-3-STUCKMTMR: Sleep with expired managed timer 62B2ABD4, time 0xE06B58 (00:00:00 ago). -Process= "Dynamic Services Timer Process", ipl= 4, pid= 40 -Traceback= 601306F0 60130B48 60283108</pre> <p>There are no known workarounds.</p>
CSCsc30505	<p>When the <b>debug pxf diversion value value</b> command is enabled, its status is not shown in the output of the <b>show debug</b> command as other IOS debugs are.</p> <p>Additionally, this debug is not disabled using the standard command forms used to disable debugs such as <b>undebg all</b> and <b>no debug pxf diversion</b>.</p> <p>Workaround: This debug may be turned off by using the <b>debug pxf diversion off</b> command.</p>
CSCsc31835	<p>A Cisco uBR10000 series CMTS may drop packets affected by the <b>service divert-rate-limit [fib-rp-glean   fib-rpf-glean] rate</b> command, when the affected packet rate is slightly slower than the specified value in the command.</p> <p>The issue only becomes easily noticeable when the rate within the command is configured at a value of 50 packets per second or higher.</p> <p>There are no known workarounds.</p>

Table 75 Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)

DDTS ID Number	Description
CSCsc31866	<p>When the <b>debug pxf diversion value</b> <i>diversion-cause</i> debug is enabled on the Cisco uBR10000 series of CMTS, the information displayed is not enough to deduce the origin of diverted packets or the packet type.</p> <p>There are no known workarounds.</p>
CSCsc32241	<p>A single tunnel interface, in a configuration of more the 1000 tunnels, does not receive the multicast traffic that it should be receiving.</p> <p>This issue occurs only in configurations with more than 1000 tunnel interfaces.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the <b>show interface</b> output are 10% of the actual packet and bit rates.</p> <p>This issue seems to occur only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsc35150	<p>If the <b>global hccp config</b> command is re-entered, the specified line card will failover.</p> <p>This issue occurs when you re-enter the <b>global hccp config</b> command and enter <b>Ctrl-Z</b> to exit. This action invokes an enter and exit at the same time and forces a line card failover.</p> <p>Workaround: To parse out the <b>config</b> command, delete the <b>config</b> command before you invoke <b>Ctrl-Z</b> or type <b>exit/end</b>. You can use <b>Ctrl-C</b> also. Either way, don't re-enter a <b>config</b> command that is already entered.</p>
CSCsc38875	<p>When a downstream cable interface on a Cisco uBR series router cable modem termination system (CMTS) experiences sustained congestion, and a significant portion of the downstream traffic is multicast traffic, Internet Group Management Protocol Version 2 (IGMPv2) Query messages might not be transmitted successfully in the downstream direction on that cable interface.</p> <p>The issue occurs when large volumes of multicast traffic, using groups that are not specified, use the cable interface <b>cable match address</b> command.</p> <p>Workaround: Ensure that all multicast traffic passing through the CMTS is classified with an appropriate <b>cable match address</b> command. This workaround may be effective only on Cisco uBR10000 series routers.</p>
CSCsc46142	<p>Modems drop offline after a line card failover.</p> <p>There are no known workarounds.</p>
CSCsc46147	<p>The Cisco uBR10000 series router unexpectedly reloads during configuration and again after a Performance Routing Engine (PRE) failover.</p> <p>There are no known workarounds.</p>
CSCsc52024	<p>Interface throughput can be reduced when an output service policy is removed.</p> <p>This issue occurs if the service policy being removed defines a bandwidth percentage on the class-default.</p> <p>There are no known workarounds.</p>

**Table 75**      **Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)**

DDTS ID Number	Description
CSCsc58767	<p>Under some circumstances on a Cisco uBR10000 series cable modem termination system (CMTS), customer premises equipment (CPE) sourced multicast traffic may not be forwarded by the CMTS to other interfaces for a brief period of time.</p> <p>To diagnose this issue, look for the temporary lack of an (S,G) entry corresponding to the CPE and multicast IP addresses in the output of the <b>show ip mroute</b> command.</p> <p>The issue occurs if the CPE is transmitting to a multicast group and then stops long enough for the expiration timer of the S,G entry in the multicast routing table to time out, but not long enough for the corresponding *,G entry to time out.</p> <p>If the CPE resumes transmission to the multicast group before the *,G entry expires, then the CMTS will not allow an S,G entry to be reinstated until the *,G entry times out.</p> <p>There are no known workarounds.</p>
CSCsc61433	<p>When multiple customer premises equipment (CPE) devices on a bundle subinterface generate multicast traffic to the same multicast group on a Cisco uBR10000 series cable modem termination system (CMTS), the CMTS will only add one of the streams to the multicast routing table as indicated by the <b>show ip mroute</b> command.</p> <p>There are no known workarounds.</p>
CSCsc62573	<p>When using the <b>clear counters</b> command to upstream ports of cable interfaces, the <b>errors</b> counter is not cleared.</p> <p>There are no known workarounds.</p>
CSCsc66340	<p>While doing repeated online insertion and removal (OIR) on the MC520S, traceback errors occur, and parallel express forwarding (PEXF) on the Performance Routing Engine (PRE) unexpectedly reloads.</p> <p>There are no known workarounds.</p>
CSCsc68251	<p>On a Cisco uBR10000 series cable modem termination system (CMTS), an error message of the following kind is generated when trying to remove fair-queueing from the class-default of a policy-map:</p> <pre>Error at ../toaster/c10k_rp/c10k_qos.c (2723) The error message may be followed by a traceback.</pre> <p>The issue may occur when removing fair-queueing from a service policy as per the following example:</p> <pre>Router(config)#policy-map test Router(config-pmap)#class class1 Router(config-pmap)#class class-default Router(config-pmap-c)#no fair-queue</pre> <p>There are no known workarounds.</p>
CSCsc71386	<p>A software-forced reload occurs while issuing CLI commands.</p> <p>There are no known workarounds.</p>

**Table 75 Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)**

DDTS ID Number	Description
CSCsc71939	<p>After a Performance Routing Engine (PRE) switchover followed by a line card (LC) switchover, if the Protect LC is reset or unexpectedly reloads, the standby PRE may crash due to a state inconsistency.</p> <p>There are no known workarounds.</p>
CSCsc73546	<p>PacketCable GATES are lost during downstream (DS) load-balancing/Dynamic Channel Change (DCC).</p> <p>There are no known workarounds.</p>
CSCsc77082	<p>The system becomes unstable when IF-MIB test is done with 536 PacketCable calls active, and in a system test environment with multiple features active on PRE2.</p> <p>This causes continuous tracebacks similar to the following:</p> <pre data-bbox="574 741 1463 1108"> 5/1: Dec 9 11:26:43.494: %IPCGRP-3-EVTOP: IPC event 400 (slot5/1): cr10k_card_send_event(): Cannot get pak buffer - dropping non-blocking ipc event -Traceback= 60483010 604AA71C 604AA7E8 600CBD1C 600CC3AC -Process= "Compute load avgs", ipl= 0, pid= 100 -Traceback= 6011BE7C 6011CB14 600B6310 600B6768 600B6ECC 60482FE0 604AA71C 604AA7E8 600CBD1C 600CC3AC 003465: Dec 9 12:01:58.835: %REQGRP-3-SYSCALL: System call for command 72 (slot5/0) : Could not send blocked IPC message (Cause: timeout) 003466: Dec 9 12:02:19.836: %REQGRP-3-SYSCALL: System call for command 72 (slot5/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 603C61F8 602BB620 602BBB50 6015B28C 60927EB0 609295EC 60926794 60C14864 60C181C0 60C086A8 60C2EC48 60601388 6060136C                     </pre> <p>There are no known workarounds.</p>
CSCsc81321	<p>The <b>vendor</b> option is missing from the <b>show cable modem</b> command. When specifying an interface, such as <b>show cable modem c4/0 vendor</b>, the <b>vendor</b> option does not work.</p> <p>Workaround: Use a command without a specific interface to get all interfaces, such as the <b>show cable modem vendor</b> command.</p>
CSCsc82827	<p>When PacketCable Multimedia (PCMM) calls are load-balanced across Mac-Domain using DCC, loss of PCMM calls and PCMM Gates occurs.</p> <p>There are no known workarounds.</p>

**Table 75 Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)**

DDTS ID Number	Description
CSCsc87181	<p>After a Performance Routing Engine (PRE) failover, the following unexpected reload occurs on the standby PRE:</p> <pre>*Dec 20 18:02:54.219: c,r=1,0, flags=0x00000010, src=0x634D88C0, dst=0x58001000, len=512 *Dec 20 18:02:54.219: -Traceback= 6010AF68 6015F5A0 6015D568 6015CC60 6015D354 6015D420 600F33EC 600F39FC 600F4568 600F03C4 6053966C 60602244 60602228 *Dec 20 18:02:54.219: c10k_ttcmm_read: Illegal access from toaster memory, state=1. *Dec 20 18:02:54.219: c,r=5,0, flags=0x00000010, src=0x634D8AC0, dst=0x5C0011DC, len=20 *Dec 20 18:02:54.219: -Traceback= 6010AF68 6015F71C 6015D568 6015CC60 6015D354 6015D420 600F33EC 600F39FC 600F4568 600F03C4 6053966C 60602244 60602228 *Dec 20 18:02:54.219: c10k_ttcmm_read: Illegal access from toaster memory, state=1. *Dec 20 18:02:54.219: c,r=4,0, flags=0x00000010, src=0x634D8AD8, dst=0x5C0013EC, len=20 *Dec 20 18:02:54.223: -Traceback= 6010AF68 6015F7B8 6015D568 6015CC60 6015D354 6015D420 600F33EC 600F39FC 600F4568 600F03C4 6053966C 60602244 60602228 *Dec 20 18:02:54.223: c10k_ttcmm_read: Illegal access from toaster memory, state=1.</pre> <p>There are no known workarounds.</p>
CSCsc91717	<p>There is a discrepancy in packet classification between Fast Ethernet and Gigabit Ethernet interfaces.</p> <p>There are no known workarounds.</p>
CSCsc98042	<p>Enabling equalizer-coefficient (known as Pre-Equalization (PRE-EQ)) on an upstream (US) port causes low signal-to-noise ratio (SNR) readings, however, it makes it difficult to troubleshoot per-house/per-modem problems for the 28U or 5x20U line cards unless one can see how the PRE-EQ is working for each modem</p> <p>Some reasons for different SNR readings for different CMs on the same plant/US port are micro-reflections, group delay, in-channel tilt. All of these issues can be focused at the house or at a specific CM location.</p> <p>Workaround: The possible workarounds are as follows:</p> <ol style="list-style-type: none"> <li>1. PRE-EQ can be disabled.</li> <li>2. Turn on PRE-EQ with the upstream (US) <b>cab ux equalization-coefficient</b> command to compensate for some of these specific modem problems and to increase SNR for specific CMs.</li> </ol>
CSCsc99862	<p>Intercept is transferred from the active to the Protect line card when a swap is performed using the <b>hccp</b> command, but intercept is not transferred to Protect line card when the <b>cable power off slot/card</b> command. is used.</p> <p>There are no known workarounds.,</p>
CSCsd03740	<p>The <b>cable upstream 0 scheduling type ?</b> command is not synchronized during an N+1 switchover.</p> <p>There are no known workarounds.</p>

**Table 75** Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)

DDTS ID Number	Description
CSCsd13114	<p>Traceback occurs on the cable modem termination system (CMTS) console during a Hot Standby Connection-to-Connection Protocol (HCCP) switchover when the Simple Network Management Protocol (SNMP) and show commands are running.</p> <p>There are no known workarounds.</p>
CSCsd20606	<p>A parallel express forwarding (PXF) restart disables multicast traffic that matches the Multicast Quality of Service (MQoS) configuration.</p> <p>This issue occurs when an MQoS configuration is applied to cable interfaces, and PXF is restarted</p> <p>There are no known workarounds.</p>
CSCsd27514	<p>Traffic on service flows with a non-zero Traffic Priority value are treated as zero priority.</p> <p>This issue occurs if there is a restart of parallel express forwarding (PXF) while the non-zero priority service flows are present.</p> <p>Workaround: Reset the affected modem.</p>
CSCsd31112	<p>Cable modems go offline when trying to load balance during an upstream channel change. Once the reset is complete, load balancing works.</p> <p>This issue occurs when load balancing is <b>dynamic</b> and baseline privacy interface (BPI) is configured at the same time.</p> <p>Workaround: Turn BPI off, or simply reset the modems.</p>
CSCsd31970	<p>On a Cisco uBR10000 series router cable modem termination system (CMTS) with redundant Performance Routing Engine (PRE) modules, new interface mode configuration commands entered on the active PRE may not be properly synchronized to the standby PRE if the <b>do show running-configuration</b> command is entered in interface configuration mode.</p> <p>This issue can lead to a configuration mismatch between the two PRE modules and can cause difficulty on PRE switchover.</p> <p>Workaround: Refrain from issuing the <b>do show running-configuration</b> command in interface configuration mode, or completely exit interface configuration mode after issuing the command.</p>
CSCsd36652	<p>When configuring line card redundancy by using the <b>global HA</b> commands, duplicate RF-switch slot numbers were configured. This configuration is not allowed.</p> <p>There are no known workarounds.</p>
CSCsd43741	<p>VID data in the entPhysicalHardwareRev MIB displays the wrong value if the data field in EEPROM is missing.</p> <p>This issue affects the Entity MIB in all Cisco uBR10000 software releases, if the VID data field is not programmed.</p> <p>There are no known workarounds.</p>

**Table 75**      **Open Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)**

DDTS ID Number	Description
CSCsd77991	<p>A line card on the Cisco uBR10000 series router unexpectedly crashes.</p> <p>This issue occurs when the <b>clear cable modem</b> command is executed for multicast address.</p> <p>Workaround: Do not use the <b>clear cable modem</b> command for multicast addresses.</p>
CSCsd95113	<p>A cable modem, when enforced with a quality of service (QoS) profile created using the cdxCmtsCmQosProfile MIB, accepts the profile and <b>show cable modem reg</b> shows the modem with the enforced profile. However, the same cable modem, after reset, does not come online with the enforced profile. Instead, it comes online with the default profile. In contrast, the same modem (when enforced with the QoS profile created using the CLI) comes online after reset with the enforced profile, not the default profile.</p> <p>This behavior is the same irrespective of platforms and whether the QoS profile is created using the CLI or the Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>
CSCse00016	<p>The PXF_Crashinfo file write operation fails to complete.</p> <p>This issue may occur due to an unscheduled restart of parallel express forwarding (PXF).</p> <p>There are no known workarounds.</p>
CSCse02543	<p>When some modems are in the reject state and a <b>clear cable modem reject delete</b> command is issued, a CM_INCONSISTENCY message is generated.</p> <p>Workaround: Do not use the <b>clear cable modem reject delete</b> command.</p>
CSCse05641	<p>Syslog messages with newlines get truncated on the syslog server and are treated as invalid.</p> <p>This issue occurs because the system event message has Message-text with a newline (\n) causing the message to be in two lines rather than a single line.</p> <p>For example, the following shows the message as seen in cable modem termination system (CMTS) logs in separate lines:</p> <pre>Apr 17 15:01:22.489 EDT: %UBR10000-3-MACADDRERR: DHCP Msg with non unicast MAC address. Master Interface Cable7/0/0 Input Interface SID = 65535 MAC = 0000.0000.0000</pre> <p>Ideally, the message should be all in one line as follows:</p> <pre>Apr 17 15:01:22.489 EDT: %UBR10000-3-MACADDRERR: DHCP Msg with non unicast MAC address. Master Interface Cable7/0/0 Input Interface SID = 65535 MAC = 0000.0000.0000</pre> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(17a)BC1

Table 76 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17a)BC1.

**Table 76** Resolved Caveats for Cisco IOS Release 12.3(17a)BC1

DDTS ID Number	Description
CSCeh69909	<p>After a line card (LC) switchover authentication, rejected modems are stuck in the init(o) state.</p> <p>This issue occurs when the modems are provisioned with privacy and Data-over-Cable Service Interface Specification (DOCSIS) 1. The same problem occurs during the switchover from protect to active.</p> <p>Workaround: Use the <b>clear cable modem mac-addr delete</b> command to make the modem come up.</p>
CSCek36686	<p>A PRE2 card unexpectedly reloads if a cable intercept configuration is added/removed for a cable modem which is transitioning between different Data-over-Cable Service Interface Specification (DOCSIS) states.</p> <p>This issue occurs when the debug cable intercept command is used.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Do not remove/adda cable intercept related configuration for a cable modem from the cable modem termination system (CMTS) while that cable modem is in a transitioning state.</li> <li>2. Do not turn on any cable intercept debugs on CMTS.</li> </ol>
CSCek26121	<p>The sysUptime SNMP OID counter is reset after a Performance Routing Engine (PRE) switchover occurs.</p> <p>There are no known workarounds.</p>
CSCek31085	<p>The interfaces.ifTable.ifEntry.ifSpeed MIB variable reports an invalid value for a 6.4 MHz, 64-QAM A-TDMA channel on a Cisco uBR10000 series router running Cisco IOS Release 12.2(15) BC2f or 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>

**Table 76 Resolved Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)**

DDTS ID Number	Description
CSCsc43642	<p>A cable modem termination system (CMTS) can experience an intermittent problem with cable modems being able to pass traffic, but not being pingable. The cable modems stay online and the customer premises equipment (CPE) behind the cable modem are pingable.</p> <p>Only cable modems are affected; the CPE IP addresses are correct.</p> <p>The following is an example of this issue:</p> <pre>Router# show cable modem a.b.c.d MAC Address      IP Address      I/F      MAC      Prim RxPwr Timing  Num BPI Offset  CPE Enb xxx.yyy.zzz  a.b.c.d      C7/0/3/U0 online  2839 -3.00 2262  1  N Router# show controllers cable 7/0/3 u 0   i SNR US phy SNR_estimate for good packets - 27.1419 dB</pre> <p>The issue is most prevalent on Cisco uBR10000 series routers.</p> <p>Workaround: Reset the modem(s) through the CLI or power cycle. The issue can sometimes disappear by itself; pinging the CPE also helps.</p>
CSCsd03006	<p>The Cisco uBR10000 series router may experience tracebacks, bus errors or system hangs during online insertion and removal (OIR) operations when OIR-compatibility is enabled.</p> <p>This issue occurs when the OIR-compatibility feature is activated on a cable modem termination system (CMTS) line card that has one or more interfaces serving as a bundle master. The issue occurs when replacing an MC5x20 card with a compatible, but not identical, MC5x20. It does not occur when a card is replaced by an identical card type or if the OIR-compatibility feature is not enabled.</p> <p>Workaround: Remove the CMTS interface from the bundle prior to performing the OIR.</p>
CSCsd12954	<p>This caveat enables cloned modem detection message to be part of SYSLOG messages.</p>
CSCsd13047	<p>The Mqos SID is not created after a line card switchover.</p> <p>This issue occurs on the interface in vib-subif mode when upstream broadcast traffic is present on the cable interfaces in the bundle.</p> <p>There are no known workarounds.</p>
CSCsd15546	<p>A Cisco router that is configured as a Dynamic Host Configuration Protocol (DHCP) relay may not append option 82 (that is, the Relay Agent option), even when the router is configured to do so in the following way:</p> <pre>ip dhcp relay information option no ip dhcp relay information check ip dhcp relay information trust-all</pre> <p>This issue occurs when the DHCP message contains an invalid option according to RFC 2132; for example, option 12 with length 0.</p> <p>Workaround: Ensure that the DHCP messages that is sent to the Cisco router functions as a DHCP relay contains valid options. If you cannot ensure this, there is no workaround.</p>

**Table 76**      **Resolved Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb16491	<p>A Cisco uBR10000 series router unexpectedly reloads when performing a <b>clear cable modem mac delete</b> while running ubr10k2-k9p6-mz.123-9a.BC3.bin.</p> <p>There are no known workarounds.</p>
CSCsc33372	<p>The following error message may appear after a cable modem termination system (CMTS) reload:</p> <pre>UBR10000-3-NOMEM: Failed to get event buffer from flap-list event chunk</pre> <p>There are no known workarounds.</p>
CSCsc55372	<p>A cable modem termination system (CMTS) unexpectedly reloads in dialer function after issuing <b>show</b> commands.</p> <p>There are no known workarounds.</p>
CSCsc96651	<p>A Cisco uBR10012 router with Policy-Based Routing and <b>set ip default next-hop</b> is not working correctly when there is a default route (0.0.0.0) in the IP routing table. Instead of selecting the PBR next-hop address, it selects and switches packets to the default route next-hop.</p> <p>This issue occurs on a Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC.</p> <p>Workaround: Remove the default route (none) from the routing table to correct the PBR next-hop selection.</p> <p>Alternative workaround: Use <b>set ip next-hop</b> to provide correct next-hop behavior.</p>
CSCsd17301	<p>With Dynamic Message Integrity Check (DMIC) configured on the cable modem termination system (CMTS), the CMTS enters a state where all subsequent cable modem (CM) registration attempts fail and the CM ends up in the in init(io) state. Cable modems that are online continue to work, but any cable modems that are reset, either by means of power-cycling or by the delete/reset CLI, do not work.</p> <p>This issue occurs if the Multi-System Operator (MSO) mistakenly provisions a modem configuration file that does not exist on the Trivial File Transfer Protocol (TFTP) server, and any modem tries to get online with CMTS using the non-existent configuration file.</p> <p>There are no known workarounds.</p>
CSCsd18928	<p>Current cable modem termination system (CMTS) code allocates and frees up large blocks of memory for various CMTS functions, which exacerbates memory fragmentation issues in large Multi-System Operator (MSO) deployments.</p> <p>There are no known workarounds.</p>

Table 76 Resolved Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)

DDTS ID Number	Description
CSCsd32249	<p>A Cisco uBR10000 cable modem termination system (CMTS) generates the following tracebacks during normal operation:</p> <pre>SCHED-3-STUCKMTMR: Sleep with expired managed timer 655717A4, time 0x280DC4750 (00:00:00 ago). -Process= "Dynamic Configfile server", ipl= 4, pid= 73 -Traceback= 605906DC 60590B34 602A4208 6056ED38 6056ED1C</pre> <p>This may be accompanied by spurious memory access:</p> <pre>%ALIGN-3-SPURIOUS: Spurious memory access made at 0x602BF6D0 reading 0x16C %ALIGN-3-TRACE: -Traceback= 602BF6D0 601865EC 602B844C 6033CCA8 6033CD28 6033C7FC 604E0EB8 6017DCD4</pre> <p>There are no known workarounds.</p>
CSCsd39040	<p>The Simple Network Management Protocol (SNMP) getmany query on the ccaHCCPGroupTrackInterfaceTable returns a partial value.</p> <p>When querying ccaHCCPGroupTrackInterfaceTable, tracklist (hp-&gt;tracklist), all of the Hot Standby Connection-to-Connection Protocol (HCCP) interfaces need to be checked. This issue occurs because of a misplaced NULL check. The tracklist of first HCCP interface is checked, but the tracklists for the other interfaces are missed.</p> <p>Workaround: Place the NULL check in the correct sequence.</p>
CSCsd42745	<p>The cable modem (CM) list is not present in the <b>show interface cable interface keyman sid multicast sid</b> output.</p> <p>This issue occurs when Authentication, Authorization, and Accounting (AAA) authorization is enabled and a line card (LC) switchover is triggered.</p> <p>There are no known workarounds.</p>
CSCsd56351	<p>A cable modem gets stuck in the init(t) state when connected to a Cisco cable modem termination system (CMTS) running Cisco IOS Release 12.3(13a)BC2.</p> <p>This issue occurs when the registered modem goes offline, and the subsequent pre-registration packet's type-of-service (ToS) field from that cable modem is overwritten using the rules of the old DOCSIS configuration file. As a result, the tftp-ack packets are dropped on the next hop router due to an unexpected TOS field in packets. For packets from an unregistered cable modem, the ToS field should not be overwritten by CMTS.</p> <p>If the <b>clear cable modem H.H.H delete</b> command is executed from cable modem termination system (CMTS), the ToS field is not overwritten by CMTS.</p> <p>Workaround: Delete the stuck cable modem from CMTS by executing the following command, which will brings the stuck cable modem back into an online state:</p> <pre>clear cable modem mac-address delete</pre>
CSCsd62061	<p>The <b>cable dynamic-flow vrf name</b> command is not seen in the running configuration after a reload, but it is still seen in the startup-configuration file.</p> <p>This issue occurs after a reload.</p> <p>Workaround: Configure <b>cable dynamic-flow vrf name</b> at the interface.</p>

**Table 76** Resolved Caveats for Cisco IOS Release 12.3(17a)BC1 (continued)

DDTS ID Number	Description
CSCsd65496	<p>A Cisco uBR router running Cisco IOS Release 12.3(9a)BC7 with 5cable-MC520s-d cards and packets generates NoSuchInstance errors when snmpget starts with ifInNUcastPkts. The ifInNUcastPkts is not populated for this ifType (docsCableUpstream) in the sparse ifTable.</p> <p>Workaround: Use snmpwalk or exclude object in the sparse ifTable (for example, ifInNUcastPkts, ifOutNUcastPkts, or ifOutQLen in snmpget).</p>
CSCsd81136	<p>After a line card switchover, one or more cable modems (CMs) are stuck in the init(i) state.</p> <p>This issue may occur if the CMs are provisioned with privacy and was observed in a DOCSIS 1.1 environment after a switch over (Working to Protect) and subsequent switch back (Protect to Working).</p> <p>Workaround: To clear up a single modem in this state, try entering the following commands:</p> <pre>clear cable modem h.h.h delete clear ip arp d.d.d.d</pre> <p>where <i>h.h.h</i> is the mac-address of the stuck CM and <i>d.d.d.d</i> is the IP address of that same CM.</p>

## Open Caveats for Release 12.3(17a)BC

[Table 77](#) lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17a)BC.

Table 77 Open Caveats for Cisco IOS Release 12.3(17a)BC

DDTS ID Number	Description
CSCee39660	<p>The cable modem termination system (CMTS) reports a traceback error during a Performance Routing Engine (PRE) switchover.</p> <p>There are no known workarounds.</p>
CSCeh48461	<p>The Performance Routing Engine (PRE) unexpectedly reloads with the following trace:</p> <pre>ubr10k2-k9p6u2-mz.2005-03-24.123BC_PI2.symbols.gz read in Enter hex value: 602A61DC 602A6360 602A6D44 60029878 60026E84 60022510 6068A464 60619A74 0x602A61DC:sch_rp_cmts_monitor_output(0x602a616c)+0x70 0x602A6360:sch_handle_headsail_pak(0x602a621c)+0x144 0x602A6D44:c10k_sch_rx_interrupt(0x602a64ac)+0x898 0x60029878:cobalt_process_to_rp_packet(0x60029500)+0x378 0x60026E84:cobalt_to_rp_interrupt(0x600268a8)+0x5dc 0x60022510:c10k_cobalt_type0_interrupt(0x600224f0)+0x20 0x6068A464:c10k_netio_intr_dispatch_post_v7(0x6068a338)+0x12c 0x60619A74:r4k_intr_dispatch(0x606199a8)+0xcc</pre> <p>This issue is observe after a line card failover and occurs when malformed packets are sent through PXF.</p> <p>Workaround: A workaround was committed under CSCsc51925. Although this does not fix the root cause of the issue, it does prevent the system from unexpected reloads.</p>
CSCeh48889	<p>The INVALIDSIDPOSITION message occurs on an interface when a large number of cable modems are going online and offline at once</p> <p>For example:</p> <pre>%UBR10000-3-INVALIDSIDPOSITION: Invalid SID (4184) position for interface Cable5/0/0: CM 00d1.1477.7451:Is used by CM 00d0.d726.ef0b SFID 6813 SID 4184. SID container info: start 744 end 6967 -Traceback= 6030A628 6030A844 6030B098 602F81FC 603A480C 605E1398 605E137C</pre> <p>One typical trigger for this message is the <b>clear cable modem delete</b> or <b>clear cable modem oui oui delete</b> command. The affected modem is kicked offline and will usually come back online later. Many different modems may be affected.</p> <p>Workaround: <b>Shut /no shut</b> the affected cable interface, or delete most modems on the cable interface.</p> <p>Alternative workaround: Reduce the number of cable modems on the affected cable interface by moving modems to other ports.</p>
CSCei22859	<p>The secondary service does not pass traffic after a line card switchover.</p> <p>This issue is likely related to payload header suppression (PHS) traffic and switchovers.</p> <p>Workaround: Do not use PHS.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are being forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>

**Table 77 Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCei54281	<p>With N+1 switchovers, the number of expected customer premises equipment (CPE) devices does not get reflected in the <b>show cable modem verbose</b> command.</p> <p>This issue occurs in a Performance Routing Engine High Availability (HA) configuration.</p> <p>There are no known workarounds.</p>
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>
CSCei69955	<p>Unsolicited Grant Services (UGS) service flows (SFs) move to the provisioned state when the channel-width and mini-slot values are changed.</p> <p>There are no known workarounds.</p>
CSCej39802	<p>An entry for an authorized mcast group is missing in the docsBpi2CmtsIpMulticastMapTable after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCej52702	<p>The active time for upstream (US) related DYN service flow resets when PacketCable calls are up for more than 5 minutes</p> <p>There are no known workarounds.</p>
CSCej89378	<p>The line card unexpectedly reloads during N+1 operation.</p> <p>There are no known workarounds.</p>
CSCek20675	<p>Support is added for the <b>show pxf cable source-verify</b> command for PRE2.</p> <p>There are no known workarounds.</p>
CSCek21720	<p>Traceback occurs with packet intercept during a line card (LC) switchover in PRE2.</p> <p>This issue occurs when the LC switchover is performed while PacketCable (PC) calls and class features are in progress.</p> <p>There are no known workarounds</p>
CSCek24075	<p>Zero nodes are reported in the <b>show srp topology</b> command.</p> <p>There are no known workarounds.</p>
CSCek25218	<p>The Spatial Reuse Protocol (SRP) interface reports the following when configuring a service policy:</p> <pre>No queue found with class id 1'set srp-priority &lt;&gt; ' failed on (side A) Interface</pre> <p>There are no known workarounds.</p>
CSCek26121	<p>The sysUptime SNMP OID counter is reset after a Performance Routing Engine (PRE) switchover occurs.</p> <p>There are no known workarounds.</p>

**Table 77**      **Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCek27678	<p>The <b>show access-lists</b> command displays the access control lists (ACLs) for deleted packet filter groups. The corresponding internal ACLs are not removed, even after the packet filter group is deleted.</p> <p>In addition, the <b>show cable filter</b> command lists the reserved ACL group 255 index 1 with drop action, even if all the cable filter configurations have been removed from the cable modem termination system (CMTS).</p> <p>There are no known workarounds.</p>
CSCin92949	<p>When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.</p> <p>This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.</p> <p>Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.</p>
CSCin95249	<p>After resetting the modem while using baseline privacy interface plus (BPI)+ enabled configurations, the line card fails to respond.</p> <p>There are no known workarounds.</p>
CSCin98031	<p>N+1 synchronization does not occur when switching over from the Working card to the Protect card.</p> <p>There are no known workarounds.</p>
CSCsb20150	<p>Under certain conditions, two Cisco uBR10000 series routers that are connected to each other over a Gigabit Ethernet medium can stop communicating bi-directionally over the link.</p> <p>The input queue and the output queue on both cable modem termination systems (CMTSs) will indicate which device is transmitting, and which device is receiving. The device having the difficulty will stop receiving on the circuit. On one of the CMTS input queues, there will be no additional packet input seen. The Cisco Discovery Protocol (CDP) will not work correctly and routing protocols will also fail. Issuing HW-RESET or shutting/unshutting the interface will not make a difference.</p> <p>This issue occurs on Cisco uBR10000 series routers running Cisco IOS Release 12.3(9a)BC3.</p> <p>Workaround: Reload the CMTS.</p>
CSCsb21814	<p>When using the downstream load balancing, utilization method, the cable modem termination system (CMTS) will load balance using the max utilization upstream (US) or downstream (DS). For example, when one interface has a max utilization on the downstream, and the other has a max utilization on the upstream, CMTS moves all US traffic to one interface.</p> <p>There are no known workarounds.</p>
CSCsb26657	<p>The toaster feed_back context rate is excessive when multicast traffic is present.</p> <p>There are no known workarounds.</p>

Table 77 Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCsb27941	<p>A PacketCable call with Three Way Calling configured is distorted /lost after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCsb27976	<p>A PacketCable call with Three Way Calling configured is distorted after a Performance Routing Engine (PRE) switchover.</p> <p>There are no known workarounds.</p>
CSCsb72639	<p>Modems are transmitting 20 dB lower than they should. The issue appears to be “gain” in the plant. The CMTS is set for 0 dBmV US input, but the actual level is -20 dBmV at the US port, and the CMTS is happy with it and does not tell the modems to transmit hotter as it should. This results in poor signal-to-noise ratio (SNR), because the CMTS noise floor may be the limiting factor.</p> <p>This issue occurs when the customer decides to use non-default connector assignments without activating the specific JIB first.</p> <p>Workaround: Install a 20 dB pad to force the modems to go higher, even though the SNR will still only report ~23 dB. However, this just masks the real issue.</p> <p>The proper procedure would be to use default connector assignments and/or be sure to activate any interfaces that are intended to move. If the “damage” is already done, perform the following:</p> <ol style="list-style-type: none"> <li>1. Determine where the connector would normally be assigned</li> <li>2. Go under that interface and assign a DS freq.</li> <li>3. Use no cab down rf-shut</li> <li>4. Use no cab u0 shut</li> <li>5. Use cab u0 frequ xxx</li> <li>6. Use cab u0 connector y (have to assign a new connector to activate this JIB since its default assignment is being used for another interface)</li> </ol> <p>This will get the specific connector out of this strange state and the CMs should transmit ~20 dB higher.</p>
CSCsb77206	<p>On a Cisco uBR10000 series router with PRE2, all downstream packets are allowed to go through, even if they match a packet filter group criteria and the match-action is to drop the packets.</p> <p>This issue occurs for both cable modem (CM) and customer premises equipment (CPE) filters in the downstream only. For upstream CM and CPE packet filter groups, the correct match-action is taken.</p> <p>There are no known workarounds.</p>

**Table 77**      **Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCsb86099	<p>While performing a switchover, the following error message occurs. After multiple switchovers, the router unexpectedly crashes:</p> <pre>Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC2 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC3 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-MAC4 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US0 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US1 Physical Port Link Down Sep 14 11:17:36.665 UTC: %ALARM-6-ENTITY_INFO: ASSERT MINOR Cable6/1-US2 Physical Port Link Down</pre> <p>This issue occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>• Performing a Route Processor Redundancy (RPR) switchover using the CLI.</li> <li>• Performing multiple switchovers</li> </ul> <p>There are no known workarounds.</p>
CSCsb93608	<p>When congestion with tail drops occurs on a downstream interface, a 15% increase in CPU utilization occurs on the 2x8 cable line card.</p> <p>There are no known workarounds.</p>
CSCsc20266	<p>Data-over-Cable Service Interface Specification (DOCSIS) TLV type 44 is incorrectly used. As a result, any modem sending a REG_REQ that includes DOCSIS TLV type 44 can not come online.</p> <p>This issue affects Cisco IOS Release 12.2(15)BC02 and all 12.3BC releases with a network that has DOCSIS 2.0 certified modems.</p> <p>There are no known workarounds.</p>
CSCsc25790	<p>Modems are not balanced across upstreams.</p> <p>This issue occurs when load balance is configured for passive mode.</p> <p>Workaround: Use static mode or dynamic mode for balancing.</p>

Table 77 Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCsc30294	<p>The following traceback occurs when testing line card failover while making a call from a Cisco uBR10000 series router.</p> <pre>Remote CMTS calls in progress CLI switchover working to protect. SLOT 5/0: Oct 25 17:25:20.871: %SCHED-3-STUCKMTMR: Sleep with expired managed timer 62B2ABD4, time 0xE06B58 (00:00:00 ago). -Process= "Dynamic Services Timer Process", ipl= 4, pid= 40 -Traceback= 601306F0 60130B48 60283108</pre> <p>There are no known workarounds.</p>
CSCsc32241	<p>A single tunnel interface, in a configuration of more the 1000 tunnels, does not receive the multicast traffic that it should be receiving.</p> <p>This issue occurs only in configurations with more than 1000 tunnel interfaces.</p> <p>There are no known workarounds.</p>
CSCsc32249	<p>Packet and bit rate statistics in the <b>show interface</b> output are 10% of the actual packet and bit rates.</p> <p>This issue seems to occur only when the configuration contains more than 2000 interfaces.</p> <p>There are no known workarounds.</p>
CSCsc34048	<p>Voice call recovery time after online insertion and removal (OIR) is more than 5 seconds. With several iterations of OIR, from Working to Protect, regular calls average a recovery time of 7 seconds. The 911 call average recovery time is 6 seconds.</p> <p>There are no known workarounds.</p>
CSCsc38875	<p>When a downstream cable interface on a Cisco uBR series router cable modem termination system (CMTS) experiences sustained congestion, and a significant portion of the downstream traffic is multicast traffic, Internet Group Management Protocol Version 2 (IGMPv2) query messages might not be transmitted successfully in the downstream direction on that cable interface.</p> <p>The issue occurs when large volumes of multicast traffic, using groups that are not specified, use the cable interface <b>cable match address</b> command.</p> <p>Workaround: Ensure that all multicast traffic passing through the CMTS is classified with an appropriate <b>cable match address</b> command. This workaround may be effective only on Cisco uBR10000 series routers.</p>

**Table 77 Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCsc43642	<p>A cable modem termination system (CMTS) can experience an intermittent problem with cable modems being able to pass traffic, but not being pingable. The cable modems stay online and the customer premises equipment (CPE) behind the cable modem are pingable.</p> <p>Only cable modems are affected; the CPE IP addresses are correct.</p> <p>The following is an example of this issue:</p> <pre>Router# show cable modem a.b.c.d MAC Address      IP Address      I/F      MAC      Prim RxPwr Timing  Num BPI Offset  CPE Enb xxx.yyy.zzz a.b.c.d C7/0/3/U0 online 2839 -3.00 2262 1 N Router# show controllers cable 7/0/3 u 0   i SNR US phy SNR_estimate for good packets - 27.1419 dB</pre> <p>The issue is most prevalent on Cisco uBR10000 series routers.</p> <p>Workaround: Reset the modem(s) through the CLI or power cycle. The issue can sometimes disappear by itself; pinging the CPE also helps.</p>
CSCsc46142	<p>Modems drop offline after a line card failover.</p> <p>There are no known workarounds.</p>
CSCsc46147	<p>The Cisco uBR10000 series router unexpectedly reloads during configuration and again after a Performance Routing Engine (PRE) failover.</p> <p>There are no known workarounds.</p>
CSCsc50111	<p>The output of the <b>show ip vrf ?</b> CLI is missing the vrf name option.</p> <p>This following is the output of the <b>show ip vrf ?</b> command:</p> <pre>Router# show ip vrf ? brief      Brief VPN Routing/Forwarding instance information detail     Detailed VPN Routing/Forwarding instance information id         Show VPN Routing/Forwarding VPN-ID information interfaces Show VPN Routing/Forwarding interface information           Output modifiers &lt;cr&gt;</pre> <p>The example is missing the following:</p> <pre>WORD      VPN Routing/Forwarding instance name.</pre> <p>The missing vrf name option also occurs with the with the following command:</p> <pre>show ip vrf [detail, interface, brief] ?</pre>
CSCsc52024	<p>Interface throughput can be reduced when an output service policy is removed.</p> <p>This issue occurs if the service policy being removed defines a bandwidth percentage on the class-default.</p> <p>There are no known workarounds.</p>
CSCsc55372	<p>A cable modem termination system (CMTS) unexpectedly reloads in dialer function after issuing <b>show</b> commands.</p> <p>There are no known workarounds.</p>

**Table 77 Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCsc58767	<p>Under some circumstances on a Cisco uBR10000 series cable modem termination system (CMTS), customer premises equipment (CPE) sourced multicast traffic may not be forwarded by the CMTS to other interfaces for a brief period of time.</p> <p>To diagnose this issue, look for the temporary lack of an (S,G) entry corresponding to the CPE and multicast IP addresses in the output of the <b>show ip mroute</b> command.</p> <p>The issue occurs if the CPE is transmitting to a multicast group and then stops long enough for the expiration timer of the S,G entry in the multicast routing table to time out, but not long enough for the corresponding *,G entry to time out.</p> <p>If the CPE resumes transmission to the multicast group before the *,G entry expires, then the CMTS will not allow an S,G entry to be reinstated until the *,G entry times out.</p> <p>There are no known workarounds.</p>
CSCsc58916	<p>When changing the access list that has been configured on a Gigabit Ethernet interface by a new one, the new access list is not denying the traffic as expected</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC7.</p> <p>There are no known workarounds.</p>
CSCsc61433	<p>When multiple customer premises equipment (CPE) on a bundle subinterface generate multicast traffic to the same multicast group on a Cisco uBR10000 series CMTS, the CMTS will only add one of the streams to the multicast routing table as indicated by the <b>show ip mroute</b> command.</p> <p>There are no known workarounds.</p>
CSCsc66268	<p>The ifAdminStatus and ifOperStatus of the Physical DOCSIS interfaces, configured as Hot Standby Connection-to-Connection Protocol (HCCP) Protect interfaces, return an invalid value of zero (0). This issue does not affect the MAC domain interface (e.g. Cable5/0/0), but only the physical layer interfaces (Cable5/0/0-upstream0).</p> <p>This issue occurs whenever an snmp get is issued for ifAdminStatus or ifOperStatus of the affected interfaces on a Cisco uBR10012 CMTS running Cisco IOS Release 12.3BC software. The interface must be configured as an HCCP Protect interface for this to occur.</p> <p>There are no known workarounds.</p>
CSCsc66340	<p>While performing repeated online insertion and removals (OIRs) on the MC520S, traceback errors occur, and parallel express forwarding (PXF) on the Performance Routing Engine (PRE) unexpectedly reloads.</p> <p>There are no known workarounds.</p>
CSCsc67630	<p>Five seconds after the <b>LC Test Crash</b> command is executed, all the PacketCable Multimedia (PCMM) calls fail.</p> <p>There are no known workarounds.</p>
CSCsc67919	<p>PacketCable calls cause the traceback cmts_get_dyn_transc_state.</p> <p>There are no known workarounds.</p>

**Table 77**      **Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCsc71386	<p>A software-forced reload occurs while issuing CLI commands.</p> <p>There are no known workarounds.</p>
CSCsc71939	<p>After a Performance Routing Engine (PRE) switchover followed by a line card (LC) switchover, if the Protect LC is reset or unexpectedly reloads, the standby PRE may crash due to a state inconsistency.</p> <p>There are no known workarounds.</p>
CSCsc73364	<p>Modems drop offline and PacketCable (PC) voice calls fail during upstream (US) load-balancing.</p> <p>There are no known workarounds.</p>
CSCsc73546	<p>PacketCable GATES are lost during downstream (DS) load-balancing/Dynamic Channel Change (DCC).</p> <p>There are no known workarounds.</p>
CSCsc74084	<p>Due to multicast packet drops and no reception of Basic SI Information and XAIT Application Information through the DOCSIS Set-Top Gateway (DSG) tunnel, the eCM in the set-top box (STB) connected to a Cisco uBR10000 series router appears to be operating in DOCSIS mode when it should be operating inDSG mode.</p> <p>Workaround: If this issue occurs, perform the following:</p> <ul style="list-style-type: none"> <li>• In the case of a bundle master (cable 5/0), remove the DSG and multicast configuration and then add them again.</li> <li>• In the case of a bundle slave, reload the module using the <b>hw-module subslot x/y reset</b> command.</li> </ul>
CSCsc77082	<p>The system becomes unstable when IF-MIB test is done with 536 PacketCable calls active, and in a system test environment with multiple features active on PRE2.</p> <p>This causes continuous tracebacks similar to the following:</p> <pre>5/1: Dec  9 11:26:43.494: %IPCGRP-3-EVTOP: IPC event 400 (slot5/1): cr10k_card_send_event(): Cannot get pak buffer - dropping non-blocking ipc event -Traceback= 60483010 604AA71C 604AA7E8 600CBD1C 600CC3AC -Process= "Compute load avgs", ipl= 0, pid= 100 -Traceback= 6011BE7C 6011CB14 600B6310 600B6768 600B6ECC 60482FE0 604AA71C 604AA7E8 600CBD1C 600CC3AC 003465: Dec  9 12:01:58.835: %REQGRP-3-SYSCALL: System call for command 72 (slot5/0) : Could not send blocked IPC message (Cause: timeout) 003466: Dec  9 12:02:19.836: %REQGRP-3-SYSCALL: System call for command 72 (slot5/0) : Could not send blocked IPC message (Cause: timeout) -Traceback= 603C61F8 602BB620 602BBB50 6015B28C 60927EB0 609295EC 60926794 60C14864 60C181C0 60C086A8 60C2EC48 60601388 6060136C</pre> <p>There are no known workarounds.</p>

**Table 77** Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCsc77238	<p>Spurious memory is seen on a Cisco uBR running Cisco IOS Release 12.3(9a)BC2.</p> <p>The spurious memory errors seems to be associated with Simple Network Management Protocol (SNMP) polling activity on the router.</p> <p>There are no known workarounds.</p>
CSCsc77514	<p>Memory usage of the CMTS SID mgmt task process keeps increasing, causing the Cisco uBR10000 series router to unexpectedly reload.</p> <p>This issue occurs when Spectrum Management is enabled on the Cisco uBR10000 series router and high memory usage observed and affects Cisco IOS Release 12.3(9a)BC7 and possibly previous releases. This issue also applies to Cisco IOS Release 12.3(13a)BC1.</p> <p>There are no known workarounds.</p>
CSCsc81321	<p>The <b>vendor</b> option is missing from the <b>show cable modem</b> command. When specifying an interface, such as <b>show cable modem c4/0 vendor</b>, the <b>vendor</b> option does not work.</p> <p>Workaround: Use a command without a specific interface to get all interfaces, such as the <b>show cable modem vendor</b> command.</p>
CSCsc82827	<p>When PacketCable Multimedia (PCMM) calls are load-balanced across the Mac-Domain using Dynamic Channel Change (DCC), loss of PCMM calls and PCMM Gates occurs.</p> <p>There are no known workarounds.</p>
CSCsc86586	<p>PacketCable (PC) calls fail upon injection of Best Effort (BE) data traffic. After data traffic starts, established PC calls start to drop.</p> <p>Workaround: Limit the number of PacketCable calls to a minimum.</p>
CSCsc87181	<p>After a Performance Routing Engine (PRE) failover, the following unexpected reload occurs on the standby PRE:</p> <pre>*Dec 20 18:02:54.219: c,r=1,0, flags=0x00000010, src=0x634D88C0, dst=0x58001000, len=512 *Dec 20 18:02:54.219: -Traceback= 6010AF68 6015F5A0 6015D568 6015CC60 6015D354 6015D420 600F33EC 600F39FC 600F4568 600F03C4 6053966C 60602244 60602228 *Dec 20 18:02:54.219: c10k_ttcmm_read: Illegal access from toaster memory, state=1. *Dec 20 18:02:54.219: c,r=5,0, flags=0x00000010, src=0x634D8AC0, dst=0x5C0011DC, len=20 *Dec 20 18:02:54.219: -Traceback= 6010AF68 6015F71C 6015D568 6015CC60 6015D354 6015D420 600F33EC 600F39FC 600F4568 600F03C4 6053966C 60602244 60602228 *Dec 20 18:02:54.219: c10k_ttcmm_read: Illegal access from toaster memory, state=1. *Dec 20 18:02:54.219: c,r=4,0, flags=0x00000010, src=0x634D8AD8, dst=0x5C0013EC, len=20 *Dec 20 18:02:54.223: -Traceback= 6010AF68 6015F7B8 6015D568 6015CC60 6015D354 6015D420 600F33EC 600F39FC 600F4568 600F03C4 6053966C 60602244 60602228 *Dec 20 18:02:54.223: c10k_ttcmm_read: Illegal access from toaster memory, state=1.</pre> <p>There are no known workarounds.</p>

**Table 77**      **Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsc90295	<p>A Cisco uBR10000 PRE1 unexpectedly reloads due to a bus error when running on a Cisco IOS Release 12.3(13a)BC1 image.</p> <p>There are no known workarounds.</p>
CSCsc94542	<p>An IP Detail Record (IPDR) stop record can randomly become missing.</p> <p>This issue occurs on the cable modem termination (CMTS) running on the Cisco IOS Release 12.3(9)BC train.</p> <p>There are no known workarounds.</p>
CSCsc96651	<p>A Cisco uBR10012 router with Policy-Based Routing using the <b>set ip default next-hop</b> is not working properly.</p> <p>A Cisco uBR10012 running Cisco IOS Release 12.3(13a)BC using the PBR with <b>set ip default next-hop</b> is not functional correctly when there is a default route (0.0.0.0) in the IP routing table. Instead of selecting the PBR next-hop address, its select and switches packets to the default route next-hop.</p> <p>Workaround: Remove default route (none) from routing table to correct the PBR next-hop selection.</p> <p>Alternative workaround: Use <b>set ip next-hop</b> to provide correct next-hop behavior.</p>
CSCsc98042	<p>Enabling equalizer-coefficient (known as Pre-Equalization (PRE-EQ) on an upstream (US) port causes low signal-to-noise ratio (SNR) readings, however, it makes it difficult to troubleshoot per-house/per-modem problems for the 28U or 5x20U line cards unless one can see how the PRE-EQ is working for each modem</p> <p>Some reasons for different SNR readings for different CMs on the same plant/US port are micro-reflections, group delay, in-channel tilt. All of these issues can be focused at the house or at a specific CM location.</p> <p>Workaround: The possible workarounds are as follows:</p> <ol style="list-style-type: none"> <li>1. PRE-EQ can be disabled.</li> <li>2. Turn on PRE-EQ with the upstream (US) <b>cab ux equalization-coefficient</b> command to compensate for some of these specific modem problems and to increase SNR for specific CMs.</li> </ol>
CSCsc99862	<p>Intercept is transferred from the active to the Protect line card when a swap is performed using the <b>hccp</b> command, but intercept is not transferred to Protect line card when the <b>cable power off slot/card</b> command. is used.</p> <p>There are no known workarounds.,</p>
CSCsd07404	<p>The <b>clear cable host</b> command is not working in PRE2 running on Cisco IOS Release 12.3.13a.BC1. All Packet Cable (PC) hosts can still send data to the external network.</p> <p>Workaround: <b>Shut</b> and <b>no shut</b> the ports, or downgrade the IOS release to Cisco IOS Release 12.3.9a.BC.</p>
CSCsd13114	<p>Traceback occurs on the cable modem termination system (CMTS) console during a Hot Standby Connection-to-Connection Protocol (HCCP) switchover when the Simple Network Management Protocol (SNMP) and show commands are running.</p> <p>There are no known workarounds.</p>

Table 77 Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCsd18928	<p>Current cable modem termination system (CMTS) code allocates and frees up large blocks of memory for various CMTS functions, which exacerbates memory fragmentation issues in large Multi-System Operator (MSO) deployments.</p> <p>There are no known workarounds.</p>
CSCsd20606	<p>A parallel express forwarding (PXF) restart disables multicast traffic that matches the Multicast Quality of Service (MQoS) configuration.</p> <p>This issue occurs when an MQoS configuration is applied to cable interfaces, and PXF is restarted</p> <p>There are no known workarounds.</p>
CSCsd24119	<p>The following error message followed by a traceback is reported by the router about once per minute:</p> <pre>%GENERAL-3-EREVENT: HW_MFIB: No shadow_mdb</pre> <p>This issue occurs when multicast is enabled.</p> <p>There are no known workarounds.</p>
CSCsd27514	<p>Traffic on service flows with a non-zero Traffic Priority value are treated as zero priority.</p> <p>This issue occurs if there is a restart of parallel express forwarding (PXF) while the non-zero priority service flows are present.</p> <p>Workaround: Reset the affected modem.</p>
CSCsd27668	<p>The Cisco uBR10000 (PRE1) experiences a parallel express forwarding (PXF) reload with following syslog messages:</p> <pre>%PXF-2-FAULT: T1 SW Exception: CPU[t1rlc1] 0x00000680 at 0x0C8D LR 0x090A %PXF-2-FAULT: T1 Exception summary: CPU[t1rlc1] Stat=0x00000002 HW=0x00000000 LB=0x00000000 SW=0x00000680 %C10KEVENTMGR-4-PXF_CRASHINFO: Writing PXF debug information to &lt;skip&gt; %C10KEVENTMGR-1-MAJOR_FAULT: PXF DMA Toaster Fault, Restarting PXF</pre> <p>This issue occurs on a Cisco uBR10000 series router with PRE1 running Cisco IOS Release 12.3(9a)BC4 and causes the Route Processor (RP) to reset.</p> <p>There are no known workarounds.</p>
CSCsd28746	<p>Unexpected values for type-of-service (ToS) and mask appear in the quality of service (QoS) profile output.</p> <p>There are no known workarounds.</p>
CSCsd31112	<p>Cable modems go offline when trying to load balance during an upstream channel change. Once the reset is complete, load balancing works.</p> <p>This issue occurs when load balancing is <b>dynamic</b> and baseline privacy interface (BPI) is configured at the same time.</p> <p>Workaround: Turn BPI off, or simply reset the modems.</p>

**Table 77** Open Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCsd31970	<p>On a Cisco uBR10000 series router cable modem termination system (CMTS) with redundant Performance Routing Engine (PRE) modules, new interface mode configuration commands entered on the active PRE may not be properly synchronized to the standby PRE if the <b>do show running-configuration</b> command is entered in interface configuration mode.</p> <p>This issue can lead to a configuration mismatch between the two PRE modules and can cause difficulty on PRE switchover.</p> <p>Workaround: Refrain from issuing the <b>do show running-configuration</b> command in interface configuration mode, or completely exit interface configuration mode after issuing the command.</p>
CSCsd32249	<p>A Cisco uBR10000 cable modem termination system (CMTS) generates the following tracebacks during normal operation:</p> <pre>SCHED-3-STUCKMTMR: Sleep with expired managed timer 655717A4, time 0x280DC4750 (00:00:00 ago). -Process= "Dynamic Configfile server", ipl= 4, pid= 73 -Traceback= 605906DC 60590B34 602A4208 6056ED38 6056ED1C</pre> <p>This may be accompanied by spurious memory access:</p> <pre>%ALIGN-3-SPURIOUS: Spurious memory access made at 0x602BF6D0 reading 0x16C %ALIGN-3-TRACE: -Traceback= 602BF6D0 601865EC 602B844C 6033CCA8 6033CD28 6033C7FC 604E0EB8 6017DCD4</pre> <p>There are no known workarounds.</p>
CSCsc10117	<p>When a cable modem termination system (CMTS) bundle interface has 100,000 Address Resolution Protocol (ARP) entries, entering interface configuration mode at that bundle hogs the CPU for 15-20 seconds.</p> <p>This issue occurs when the bundle interface has a large number of entries in the ARP and Forwarding Information Base (FIB) tables.</p> <p>Workaround: Enter bundle interface configuration mode during a maintenance window, or split one large bundle into several smaller bundle.</p>
CSCsc27520	<p>When the Network Time Protocol (NTP) clock gets updated, the clock on the Performance Routing Engine (PRE) changes as expected, however, the MC520 clock does not get updated.</p> <p>Workaround: Restart the cable modem termination system (CMTS) or the line card.</p>

## Resolved Caveats for Release 12.3(17a)BC

Table 78 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(17a)BC.

Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC

DDTS ID Number	Description
CSCea14522	<p>The following error message appears after inserting the <b>ip route W.X.Y.Z M.A.S.K CableP/Q/0.R S.T.U.V</b> command into the VPN configuration:</p> <pre>%GENERAL-3-EREVENT: HWCEF: Loadinfo fastadj lock with NULL fasttag_rew -Traceback= 600E4B14 600E3490 60405FE0 604064A8 60D5E748 60D5938C 60E32D14 60D59604 60E2F724 60E2F9F0 60DE8A84 60DE8B2C 60E224F4 60E22B50 60DF30B4</pre> <p>This issue occurs on a Cisco uBR10000 CMTS with PRE2 running Cisco IOS Release 12.3(9a)BC7.</p> <p>There are no known workarounds.</p>
CSCef60659	<p>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).</p> <p>These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:</p> <ol style="list-style-type: none"> <li>1. Attacks that use ICMP “hard” error messages</li> <li>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</li> <li>3. Attacks that use ICMP “source quench” messages</li> </ol> <p>Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.</p> <p>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</p> <p><a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050412-icmp">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050412-icmp</a></p> <p>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</p> <p><a href="http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.pdf">http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.pdf</a></p>
CSCef28979	<p>If the host IP address is changed after the cable modem is online, the host IP address is not synchronized to the standby Performance Routing Engine (PRE) or Protect line card (LC).</p> <p>This cause delays in traffic recovery after a PRE or LC switchover.</p> <p>There are no known workarounds.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCeg25277	<p>The primary Performance Routing Engine (PRE) on a Cisco uBR10000 platform unexpectedly reloads in docsis classifier code.</p> <p>If there is secondary PRE, the secondary takes over and all the cable line cards get connected to the secondary PRE. No cable modems go offline and service is restored as soon as routing converges on the WAN interface.</p> <p>There are no known workarounds.</p>
CSCeg74394	<p>The primary and backup FastEthernet (FE) or GigabitEthernet (GE) interfaces go into admin shutdown after a reload.</p> <p>While the router is coming backup after a reload, the console display Ethernets coming up and then going down, followed by a “shutdown” notice under the configuration for both interfaces.</p> <p>This issue only occurs if a higher number FE or GE interface, such as FE0/3 or GE0/3, is configured as primary while a lower number interface, such as FE 0/2 or GE0/2, is configured as backup.</p> <p>This issue does not occur when the situation is reverse: when a lower number Ethernet interface is configured as primary and a higher number Ethernet interface is configured as backup.</p> <p>In addition, one of the Ethernet interfaces will lose its configured IP address and will display “no ip address” instead in the interface configuration.</p> <p>There are no known workarounds.</p>
CSCeh13489	<p>A router may reset its Border Gateway Protocol (BGP) session.</p> <p>This issue occurs when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.</p> <p>Workaround: Configure the <b>bgp maxas limit</b> command in such a way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.</p>
CSCeh18798	<p>The cable modem termination system (CMTS) reports a Process Thrashing error during modem registration.</p> <p>There are no known workarounds.</p>
CSCeh64171	<p>After Performance Routing Engine (PRE) switchover, the cable qos profile created by the cable modem is lost. A <b>clear cable modem reset</b> to let the cable modem re-register is unsuccessful.</p> <p>This issue occurs on PRE switchover.</p> <p>Workaround: Enter the <b>clear cable modem all reset</b> command to get the qos profile back.</p>
CSCeh89315	<p>The counters for the leasequery-filter do not get cleared when <b>clear counters</b> or <b>clear counters cable x/y</b> is issued after the leasequery-filter related CLI have been un-configured.</p> <p>There are no known workarounds.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCei03655	<p>911 calls will get rejected if no single existing normal voice call can be freed to fit 911.</p> <p>Workaround: Ensure that normal voice calls for quality of service (QoS) parameters can fit 911.</p>
CSCei11912	<p>After a line card switchover, existing or new PacketCable calls do not work in an Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) environment.</p> <p>This issue occurs because the dynamic service flow ID (SFID) to VPN mapping is lost after a switchover. Hence, when dynamic service flows are created for new calls (after switchover), they get mapped to the VPN of either the cable modem or the Media Terminal Adapter (MTA), instead of the value that was configured in the configuration file or the CLI.</p> <p>There are no known workarounds.</p>
CSCei21446	<p>The <b>no cable modulation-profile grpnum</b> command has three possible actions. If the group is a default group, it is reset to the default configuration; if the group is an existing non-default group, it is cleared from internal database; if the group is a non-existing group, the empty database entry is cleared again, which has no effect.</p> <p>The issue is that there is no message printout to indicate which action is taken, causing confusion to the user.</p> <p>There are no known workarounds.</p>
CSCei25282	<p>The line card reports a keepalive error and unexpectedly reloads.</p> <p>There are no known workarounds.</p>
CSCei29988	<p>The Hot Standby Connection-to-Connection Protocol (HCCP) global configuration reports errors after a reload.</p> <p>Workaround: Configure a default RF switch DNS name.</p>
CSCei30667	<p>The <b>show cable modem vendor summary</b> CLI command produces no output:</p> <pre data-bbox="573 1341 1341 1415"> Router# show cable modem vendor summary Vendor      OUI                Cable Modem                 Total  Registered Unregistered Offline </pre> <p>This issue occurs when the modem Organizational Unique Identifier (OUI) database has more than 250 different OUI entries.</p> <p>Workarounds: Use the <b>show cable modem vendor</b> command to capture the information, and perform a sort/count using an external device such as a Packet Cable (PC) or UNIX box.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCei31900	<p>Modems using Baseline Privacy Interface Plus (BPI+) issue the following message and end up in the reject(pk) state.</p> <pre>AUTH_REJECT_PERMANENT_AUTHORIZATION_FAILURE</pre> <p>When the modem is individually reset using the <b>clear cable modem mac-address reset</b> command, it comes online(pt) without any other changes:</p> <pre>%UBR10000-3-AUTH_REJECT_PERMANENT_AUTHORIZATION_FAILURE: &lt;132&gt;CMTS [DOCSIS]:&lt;66030108&gt; Auth Reject - Permanent Authorization Failure . CM Mac Addr &lt;0004.bdaa.0000&gt;</pre> <p>This issue occurs when modem registration rates above 30 per second are sustained, more than 5000 modems are coming online at once, and high CPU usage (of over 50%) is occurring.</p> <p>In addition, trail drops may occur in the cable downstream default queues, and/or to the Route Processor (RP) queues.</p> <p>Workaround: After a cable modem termination system (CMTS) reload, or when this issue occurs, enter the following command:</p> <pre>clear cable modem reject delete</pre>
CSCei32426	<p>When a <b>write memory</b> command is executed while the Protect cable line card interface has assumed the configuration of the Working cable line card interface during a Hot Standby Connection-to-Connection Protocol (HCCP) switchover, the configuration is saved. This functionality causes a problem on the next reload because it results in conflicting configurations (such as overlapping IP addresses between the Protect line card interface and the Working line card interface).</p> <p>The non-HCCP related configuration on the Protect line card interface should not be saved when a <b>write memory</b> command is issued while it is the active interface.</p> <p>There are no known workarounds.</p>
CSCei43076	<p>Deleting a cable modem termination system (CMTS) subinterface or reading the ifTable after a CMTS line card has been reset causes a spurious memory access if the line card had one or more subinterfaces registered in the ifTable at the time of the reset.</p> <p>Workaround: Manually delete the subinterfaces prior to resetting the line card and put them back after the reset.</p>
CSCei45607	<p>The <b>service-policy</b> command is configurable on cable interfaces, which suggests to customers that Modular QoS (MQC) is supported, but MQC is currently not supported on Cable interfaces</p> <p>There are no known workarounds.</p>
CSCei46082	<p>Invalid signal-to-noise ratios (SNRs) are displayed as very high values (for example, over 1000).</p> <p>This extremely rare issue is only known to occur on the new 520T card under stress tests involving Spectrum Management. It might also occur on the Transam card.</p> <p>There are no known workarounds. This is an occurrence.</p>

Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCei54145	<p>After quality of service (QoS) enforcement and a modem reset, the modem takes the recently created profile and not the qos profile that was in use before the modem reset.</p> <p>There are no known workarounds.</p>
CSCei54307	<p>Traceback and alignment errors occur when executing <b>show pxf cpu queue</b>.</p> <p>There are no known workarounds.</p>
CSCei54858	<p>When all l2-vpn configuration is removed from one Ethernet interface, the skip af check flag will be cleared and causing other l2vpn service to other Ethernet interface.</p> <p>There are no known workarounds.</p>
CSCei55459	<p>The queue-limit configured for a policy-map is not reflected in the configuration applied. The value always remains zero.</p> <p>This issue is specific to the PRE1.</p> <p>There are no known workarounds.</p>
CSCei61732	<p>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.</p> <p>Cisco has made free software available that includes the additional integrity checks for affected customers.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-timers">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-timers</a></p>
CSCei66602	<p>The line card unexpected reloads when load balancing is enabled.</p> <p>There are no known workarounds.</p>
CSCei72559	<p>If the <b>cable modem qos profile</b> command is issued without the <b>[no-persistence]</b> option, the enforced quality of service (QoS) profile does not remain in force for cable modems across reboots. The QoS profile should remain. The <b>no-persistence</b> option does not display in the CLI help(?).</p> <p>This issue occurs on Cisco IOS Release 12.3(13a)BC</p> <p>Workaround: Use the <b>clear cable modem xxxx delete</b> command to return the original CM-created profile</p>
CSCei73998	<p>The downstream (DS) secondary service flow (SF) is not removed from the standby Performance Routing Engine (PRE) if the SF is deleted when it is in the reserved state.</p> <p>This issue occurs when a PC voice call is put on hold and then the call is terminated while on hold.</p> <p>There are no known workarounds.</p>
CSCei77416	<p>The cable modem termination system (CMTS) unexpectedly reloads when a deleted bundle interface is re-initialized with an existing configured subinterface.</p> <p>There are no known workarounds.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCei77471	<p>After multiple Hot Standby Connection-to-Connection Protocol (HCCP) switchovers, the PROTECT line card (LC) unexpectedly reloads when it becomes active. This issue occurs because the underlying Station Maintenance allocated for the virtual upstreams are not deallocated when the Protect LC is in standby mode, causing instability when the Protect LC switches back to active.</p> <p>When this issue occurs, the LC unexpectedly reloads and the modems on that LC then become offline until the Working LC takes over and gets back in service.</p> <p>Workaround: Remove and do not support virtual upstream channels per Working LC interfaces.</p>
CSCei81799	<p>The HCCP 7+1 global configuration feature (introduced in Cisco IOS Release 12.3(13a)BC has swapped the definitions of rfs1 and rfs2. This is not consistent with the existing <i>RF Switch Configuration Guide</i>.</p> <p>If US10-US23 are shutdown and U0-U9 are switched over, all modems will go offline.</p> <p>Workaround: Change the IP addresses of rfs1 and rfs2 using <b>ip host rfs# ip-address</b>.</p>
CSCei83154	<p>The OIR-compatibility feature is disabled if a secondary Performance Routing Engine (PRE) is installed.</p> <p>The presence of a secondary PRE in standby mode disables the OIR-compatibility setting.</p> <p>Workaround: Shutdown the secondary PRE before upgrading from an MC520S to an MC520u.</p>
CSCei86348	<p>The Route Processor (RP) unexpectedly reloads with the use of particular configuration file.</p> <p>There are no known workarounds.</p>
CSCei87863	<p>With Multicast Baseline Privacy Interface Plus (BPI+) enabled, multicast BPI+ streams may be refused by cable modems after the change of the access-list used for some BPI+ multicast groups because the MSAID/BPI_KEYS may be changed.</p> <p>This issue occurs if the configuration of an access-list, which is used in the <b>cable match ... bpi-enable</b> command, is change.</p> <p>Workaround: Reset the cable modem or the customer premises equipment (CPE) leaves the igmp group for several minutes. Or, instead of modifying existing ACL, add a new ACL with new cable match command.</p>
CSCej11528	<p>After reload of the cable modem termination system (CMTS), an access control list (ACL) used by the cable monitor is not sent to the cable line card from the Network Processing Engine (NPE) or the Performance Routing Engine (PRE).</p> <p>This issue occurs when CMTS reloads.</p> <p>Workaround: Unconfigure the cable monitor ACL CLI. Then configure the ACL. Then go back to the cable interface and configure the CMON:ACL CLI again. This time the CLI will be sent to the cable line card.</p>

Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCej11541	<p>Bidirectional cable monitor ACL sniffing is not filtering data correctly. When data should have been blocked due to filtering, the data is being sent to the sniffer.</p> <p>This issue only occurs when bidirectional cable monitor ACL sniffing is enabled. Incoming and outgoing directions with same ACL filter OK.</p> <p>Workaround: If-console to the cable line card (CLC). The ACL has not reached the CLC. Please configured the ACL by hand on the CLC and then exit the if-console session. Now ACL data will filter properly.</p>
CSCej18695	<p>Some access control lists (ACLs) are not being deleted on the cable line card (CLC) after the NPE/Performance Routing Engine (PRE) issued a delete to the CLC. Also, extended ACL are received corrupted at the CLC.</p> <p>Workaround: Please if-console to the CLC and delete the ACL by hand using the ACL delete CLI on the CLC, or configure an extended ACL by hand on the CLC after deleting the garbage extended list on the CLC.</p> <p>If-console is a service internal command. You have to enable service internal on the CMTS first.</p> <p>Use <b>if-con slot/subslot</b> for line cards in a Cisco uBR10000 chassis.</p>
CSCej18858	<p>A Performance Routing Engine (PRE) can wrongly timeout a line card when it should not because of a logical bug in the OIR state machine.</p> <p>This issue has been observed on a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCej22163	<p>In a high availability configuration with multiple Performance Routing Engines (PREs), the standby PRE occasionally reloads when a card is removed from the active PRE's running configuration.</p> <p>The following command sequence is an example of the type of configuration changes that might cause the error to occur.</p> <pre>Router# <b>config t</b> Router(config)# <b>card 8/1 5cable-mc520s-d</b> Router(config)# <b>no card 8/1.</b> Router(config)#</pre> <p>There are no known workarounds.</p>
CSCej28478	<p>Committed gate is stuck and freed by CMTS in special CFNA call behavior by MTA. It can use up gate resource per subscriber and cause no further gate creation allowed per such subscriber.</p> <p>Workaround: Issue a <b>clear packetcable gate all</b>. But this has an effect on clearing all gates on CMTS.</p>
CSCej30053	<p>When an extended ACL is configured for a specific host, cable monitor still filters all the traffic on the subnet of the specific host.</p> <p>This issue occurs under normal working conditions for cable monitor.</p> <p>There are no known workarounds.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCej35149	<p>When a named ACL used by cable monitor is deleted from RP card (NPE/Performance Routing Engine (PRE)), the cable line card (CLC) is supposed to delete the named ACL, but the CLC does not.</p> <p>This issue occurs under normal operation conditions.</p> <p>There are no known workarounds.</p>
CSCej37351	<p>Root Certs on Disk2 does not work.</p> <p>Workaround: The only place root certs can work is Disk1, Slot0: and Slot1:</p>
CSCej45500	<p>A cable modem attempting to come online with incorrect BPI+ credentials displays the following message in the log:</p> <pre>SLOT 8/1: Oct 12 01:30:02.039: %UBR10000-3-MANUFACTURE_CA_CM_CERTIFICATE_FORMAT_ERROR: &lt;133&gt;CMTS [DOCSIS]: Manufacture CA Certificate Format Error</pre> <p>Workaround: For large systems, there are no known workarounds. It is very unlikely that the offending modem can be located without the MAC address information and broad based modem debug messages are likely to overwhelm the system and might cause an unexpected reload or Performance Routing Engine (PRE) failover.</p> <p>For small systems, perform the following:</p> <ol style="list-style-type: none"> <li>1. Look for modems failing to come online, in reject states, or not in online(pt) online(pk) and attempt to remove that modem from the network, or issue a DOCSIS 1.0 configuration file.</li> <li>2. Then try to code upgrade that modem.</li> </ol> <p>Enable debug messages for BPI+.</p>
CSCej61240	<p>The following “% Ambiguous command:” messages were seen when IP-related commands were input:</p> <pre>% Ambiguous command: "ip dhcp pool " % Ambiguous command: "ip dhcp binding " % Ambiguous command: "ip dhcp smart-relay " % Ambiguous command: "ip domain " % Ambiguous command: "ip domain-lookup " % Ambiguous command: "ip address-pool " % Ambiguous command: "ip telnet comport "</pre> <p>This issue occurs in 12.3 BC train.</p> <p>There are no known workarounds.</p>
CSCej63139	<p>If there is no secondary RKS server specified in gate-set, traceback will occur where NULL ptr is accessed. This can cause random reload on the system due to invalid memory access.</p> <p>Workaround: Specify the secondary RKS server in CA configuration.</p>

**Table 78**      **Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCej65202	<p>The standby Performance Routing Engine (PRE) unexpectedly reloads when the active PRE attempts to configuration sync the Hot Standby Connection-to-Connection Protocol (HCCP) Protect Interdb to it. This issue is specific to configuring sub-interfaces.</p> <p>When this issue occurs, the standby PRE will recover and return to HOT Standby mode. This does not affecting service on the active PRE.</p> <p>There are no known workarounds.</p>
CSCej66025	<p>When DS BW is saturated and no more CIR queue can be allocated on toaster, a new PacketCable Multimedia (PCMM) gate will be left in the committed state and use up gate resource.</p> <p>There are no known workarounds.</p>
CSCej68481	<p>Traceback and random Performance Routing Engine (PRE) reloads occur during LC switchover with PacketCable call having CALEA wiretap turned on.</p> <p>Workaround: Turn off CALEA wiretap.</p>
CSCej71974	<p>On Cisco uBR10000 series router, the cable line card IPC may suddenly pause or hang for seconds, but the under layer IOS IPC still works. When this pause or hang is long enough, particular when the Performance Routing Engine (PRE) or BPE is busy, PRE will detect Cable line card timeout.</p> <p>This only occurs on the cable line card. Other line cards in Cisco uBR10000 series router seem to work correctly.</p> <p>There are no known workarounds.</p>
CSCej77130	<p>If you make a cable interface configuration change while an Hot Standby Connection-to-Connection Protocol (HCCP) static sync is occurring, this may cause an unexpected Performance Routing Engine (PRE) reload.</p> <p>Workaround: Wait until HCCP static sync is complete.</p>
CSCek03346	<p>Late Voice packets are observed to be further delayed, causing voice quality degradation.</p> <p>There are no known workarounds.</p>
CSCek06198	<p>Voice flows are shaped to their maximum configured bandwidth. This may shape voice packets arriving in a burst and cause voice quality degradation.</p> <p>There are no known workarounds.</p>
CSCin90684	<p>The problem occurs when enforcing the SNMP-created QoS profile to a cable modem.</p> <p>The profile does not get enforced under the following conditions:</p> <ul style="list-style-type: none"> <li>• When the profile is SNMP or CM created.</li> <li>• When the profile is updated through SNMP</li> </ul> <p>Workaround: Assign either default (3044), or any required value to max-ds-burst for that QOS profile, through the <b>cable qos prof prof-index max-ds-burst value</b> CLI before enforcing the QOS profile to the modem.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCin94417	<p>For cdxCmtsCmDMICLockQos MIB, SNMP get shows only 0 for all values which set through SNMP set.</p> <p>There are no known workarounds.</p>
CSCin95131	<p>Protector interface’s modem entries would not be there in the docsIfCmtsMacToCmTable after multiple RPR/N+1 switchovers.</p> <p>There are no known workarounds.</p>
CSCin97099	<p>Modems with an enforced QoS profile go offline after switchover.</p> <p>There are no known workarounds.</p>
CSCin97360	<p>Traffic through Transparent LAN Service (TLS) tunnel fails after a Performance Routing Engine (PRE) switchover.</p> <p>Workaround: Disable and re-enable TLS configuration after PRE switchover.</p>
CSCsa50929	<p>The Fix for CSCsa48673 will cause US Load Balancing to not decrement the Pending count.</p> <p>There are no known workarounds.</p>
CSCsa59600	<p>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).</p> <p>These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:</p> <ol style="list-style-type: none"> <li>1. Attacks that use ICMP “hard” error messages</li> <li>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</li> <li>3. Attacks that use ICMP “source quench” messages</li> </ol> <p>Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.</p> <p>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.</p> <p>This advisory is posted at</p> <p><a href="http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml">http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml</a>.</p> <p>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</p> <p><a href="http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.pdf">http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.pdf</a></p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCsb02318	<p>The following Hot Standby Connection-to-Connection Protocol (HCCP) configuration commands may not preserve their non-default configuration values after two Performance Routing Engine (PRE) switchovers unless the running-configuration is saved to startup-configuration before PRE switchover.</p> <pre data-bbox="613 457 1117 611"> [no] hccp x authentication [no] hccp x revertive [no] hccp x reverttime [no] hccp x timers [no] hccp x track                 (here x: groupnumber )                     </pre> <p>Assume that PRE-A is active PRE and PRE-B is standby PRE. When a switchover from PRE-A to PRE-B happens, PRE-A will be reset and rebooted. After rebooting, during the configuration, PRE-B will send its running-configuration over to PRE-A. This running-configuration will become PRE-A's startup-config. PRE-A will try to parse this configuration and start applying it. If the running-configuration on PRE-A was not saved before switchover, the user configured values of these commands will be absent.</p> <p>Workaround: Save the running-configuration to startup-configuration whenever the above commands are issued. This restriction will be relaxed in the next release.</p>
CSCsb02366	<p>QoS Prov for DOCSIS 2.0 cable modems correctly shows DOCSIS 1.0 or DOCSIS 1.1 because of the fact that the major difference between a modem running in DOCSIS 2.0 mode as opposed to DOCSIS 1.0/1.1 mode is the physical layer and not the QoS provisioning.</p> <p>However, to be consistent, the “DOC2.0” column should be removed from under “QoS Provision” in the <b>show cable modem mac summary</b> display.</p> <p>In additionally, the <b>show cable modem phy summary</b> display should provide a quick summary of the cable modems in each phy mode on each interface.</p>
CSCsb40202	<p>The current implementation of cable filter groups can allow a CM or customer premises equipment (CPE) device to bypass filters.</p> <p>There are two cases where this issue can be triggered:</p> <ol data-bbox="581 1339 1474 1541" style="list-style-type: none"> <li>1. MSO configures the CMTS with default cable filter groups with the <b>cable submgmt default filter-group</b> command and points them to a group ID that does not exist. IOS will not give a warning, and the device is completely open.</li> <li>2. DOCSIS1.1 provisioned CMs have TLV 37 configured, but points to a group ID that does not exist. IOS gives no warning, and the device is completely open.</li> </ol> <p>In cases where a group ID does not exist, default behavior of IOS should probably be a “deny all” like traditional ACLs instead of the current “permit all”.</p> <p>There are no known workarounds.</p>
CSCsb04892	<p>There are missing fields for 2.0 data when doing <b>show cable modem mac summary total</b>.</p> <p>This issue occurs when calling the <b>show cable modem mac summary total</b> command</p> <p>There are no known workarounds.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb05747	FLAP-LIST is not aging properly in 12.3BC. There are no known workarounds.
CSCsb14196	DSG DCDs are not flowing out the cable interface as they should be when configured.  If you look at the LC configuration via ITS console you find that the configuration for DSG and everything else that is in the global portion of the config during reload, the maximum number of global CLIs to be downloaded to the line card is 4096.  There are no known workarounds.
CSCsb15411	PacketCable calls may fail, or downstream service flows with a minimum reserved rate component may fail to be established. The failure will be accompanied by a log message similar to the following:  %UBR10000-4-DSA_UNSPECIFIED_REASON: <133>CMTS [DOCSIS]:<83000100> Service Add rejected - Unspecified reason. CM Mac Addr <000a.c4df.2222> This issue may occur when downstream admission control is unconfigured or removed from the CMTS configuration with the command <b>no cable admission-control ds-bandwidth voice arguments</b> .  Workaround: Reapplying downstream admission control with the command <b>cable admission-control ds-bandwidth voice arguments</b> will work around the problem.  In addition, a system reload will also clear this issue.
CSCsb16399	When service policy containing CBWFQ and random-detect on default queue is removed from the interface, tracebacks and assertion failures result.  This issue occurs when the policy-map contains at least one bandwidth/priority action (with or without random-detect) and default queue has a random-detect action configured on it.  There are no known workarounds.
CSCsb17060	The default cable modulation profile does not appear within the <b>show running-config</b> command even though the <b>cable modulation-profile</b> command is apparently configured.  Workaround One: Configure the <b>cable modulation-profile initial</b> command.  Workaround Two: Configure the <b>cable modulation-profile</b> command with no values.
CSCsb17673	After performing multiple Performance Routing Engine (PRE) switchovers, several of the Protect and Working LCs may go into a non-functional state.  Workaround: Reset the LC affected.
CSCsb19710	Adding the Hot Standby Connection-to-Connection Protocol (HCCP) config to an interface that is running DSG stops the DCDs from being transmitted immediately.  There are no known workarounds.

Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCsb20032	<p>After <b>shut</b> of an interface and then removal of legacy HA commands from the <b>shut</b> interface, a Performance Routing Engine (PRE) failover was performed from PREA --&gt; PREB. It was observed that after a PRE switchover, the corresponding PROTECT interface is now in *ACTIVE* state.</p> <p>There are no known workarounds.</p>
CSCsb21988	<p>When using file mode of SAMIS, the XML data appears corrupted.</p> <p>There are no known workarounds.</p>
CSCsb23279	<p>The QID for the default queue on the Cable downstream interface is not correct. Depending on its value, the symptoms may vary.</p> <p>If the microcode for the Toaster should be reloaded, either manually via CLI or dynamically via a reset, this problem will persist.</p> <p>Workaround: Do not intentionally reload the microcode. Dynamic reloads cannot be avoided.</p>
CSCsb25918	<p>On the MC520s card, signal-to-noise ratio (SNR) values may drop on a upstream causing modems to drop offline. They are running 16 QAM on the upstream.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC1 with multiple MC520s cards. Switching modulation from 16-QAM to QPSK and back restored the SNR levels</p> <p>The Init Mtn Slots were increasing. Utilization on the upstreams did not differ.</p> <p>Workaround: Disable eq-coefficient, change modulation to qpsk, revert back to 16qam and re-enable eq-coefficient.</p>
CSCsb26818	<p>When the interfaces of a newly added 5X20S card are activated, the modulation on US3 may change automatically to QPSK, even though 16QAM modulation profile is applied to it. This happens on systems without any dynamic modulation feature configured.</p> <p>This issue occurs when a 16QAM modulation profile was added to the US ports of a newly activated Cable interface on 5X20.</p> <p>Workaround: Simply re-config <b>cable upstream us-port modulation profile-number</b> again.</p>
CSCsb26840	<p>Packet drops on voice calls with PHS enabled when the maximum rate (MIR) for the voice stream is very close to the actual bandwidth used. You can notice this by picking up the phone and pressing a button. If you hear very short periods of silence interrupting the tone, that's it. Also, you can see if there are drops on the service flow by doing a <b>show interface cx/y/z service-flow n counters verbose</b> for the service flow corresponding to downstream voice data.</p> <p>This issue occurs when PHS is enabled.</p> <p>Workaround: Turn off PHS or use cable modems which have large maximum rates (MIR) for voice data.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCsb27991	<p>After configuring the CMTS with GLOBAL HA commands, and then changing the Protect line card from a 5x20s to 5x20u, not all the GLOBAL HA commands are removed from the interface.</p> <p>The expected behavior is to have all interface commands removed when changing card types. A <b>show hccp brief</b> command will not show any Protect interfaces, however, when trying to reconfigure the Protect interface the following message will be displayed:</p> <p>Subslot 5/1 is configured as Protect. To change, un-configure it first</p> <p>Workaround: Perform the following:</p> <ul style="list-style-type: none"> <li>• Unconfigure global HA commands from the interface.</li> <li>• Reconfigure global HA command on the interface</li> <li>• Save the configuration</li> </ul>
CSCsb28546	<p>Voice RTP/UDP packets are not forwarded to CALEA DF (Server) after Line Card or Performance Routing Engine (PRE) switchover is performed.</p> <p>There are no known workarounds.</p>
CSCsb30263	<p>The E911 call stays connected after line card switchover, the E911 call was lowered to a regular active call from an ActiveHiPriCall.</p> <p>There are no known workarounds.</p>
CSCsb30593	<p>Per-modem downstream packet classifiers greater than 10 do not count matching packets.</p> <p>This issue only occurs when there are more than 10 packet classifiers on a single modem, a very rare configuration.</p> <p>There are no known workarounds.</p>
CSCsb30694	<p>Repeated pxf unexpected reloads are observed with %PXF-2-FAULT: T1 Exception summary: CPU[t1r1c1]</p> <p>This occurs on a Cisco uBR10000 series router with a PRE1 platform running Cisco IOS Release 12.3(9a)BC3.</p> <p>There are no known workarounds.</p>
CSCsb31586	<p>A Cisco uBR10000 series CMTS may not deliver the required throughput to a downstream service flow.</p> <p>The issue will only occur when there are a very large number cable modems and existing downstream service flows present on the Cisco uBR10000 series router. Typically, at least 40000 downstream service flows need to be present for the issue to occur.</p> <p>The issue will only occur for new service flows created after the initial 40000 are established.</p> <p>There are no known workarounds.</p>

**Table 78** *Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb37557	<p>The term SNR in <b>show cable modem phy</b> and <b>show controller</b> is easily confused with CNR by customers.</p> <p>This issue occurs when running command <b>show cable modem phy</b> and <b>show controller</b>.</p> <p>There are no known workarounds.</p>
CSCsb37635	<p>CMTS unexpectedly reloads while the standby RP is loading.</p> <p>There are no known workarounds.</p>
CSCsb40738	<p>A Cisco uBR10000 series router may have a large number of spurious ARP entries with IP address in the range 127.64.0.0/10 or 127.128.0.0/10 in its ARP table. One source of this issue is due to the “ip proxy-arp” being applied by default to the backplane ethernet interface.</p> <p>This issue occurs when an ARP table would have large number of entries in 127.x.x.x range. This is the default configuration for the back plane ethernet interface.</p> <p>Workaround: This issue can be avoided by having an access list blocking all the traffic to and from 127.x.x.x ip addresses</p>
CSCsb42361	<p>A Cisco uBR10000 series CMTS may suffer from high CPU in the IP Background process after adding a secondary IP address to a cable or bundle interface.</p> <p>The issue may occur when the number of ARP entries on the interface being configured is in the order of tens of thousands.</p> <p>The number of ARP entries on each interface may be approximately gauged with the following command:</p> <pre>show adjacency summary</pre> <p>Workaround: Ensure that secondary IP addresses are added during a maintenance window.</p> <p>Alternative workaround: Segment the CMTS into small cable interface bundle groups or to use separate subinterfaces so that a lower number of modems and Customer Premise Equipment ARP entries are linked to each subinterface.</p>
CSCsb42820	<p>5x20 line card is hanging in the “check_flap_list” function (%LCINFO-4-LCHUNG) causing a “power cycle” (%UBR10K-1-POWCYCLE).</p> <p>Workaround: Turn off all debugs, or excessive SNMP management of the system, to reduce the size of the flap list to 4000, and change the power-adjustment threshold to 4-6 dB.</p> <p>Alternative workaround: Enter <b>no logging console guaranteed</b> on the RP and each line card.</p>
CSCsb43435	<p>The micro reflections column in the <b>show cable modem remote-query</b> command is not accurate.</p> <p>There are no known workarounds.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCsb53506	<p>Service flows that specify a max latency parameter may get less bandwidth than expected.</p> <p>If the max latency is specified (non-zero) and the minimum reserved rate is not perfectly divisible by 8000, the remainder of the division is not accounted for and the policer associated with the service flow's queue will rate limit packets at a rate below the minimum reserved rate.</p> <p>This can have a significant impact to voice flows as 10% of packets will be rate limited and voice quality will be lower than expected.</p> <p>PRE2 engine, not PRE1 max latency, must be non-zero minimum reserved rate must not be perfectly divisible by 8000.</p> <p>For example, if the standard bit rate of 87,200 bps for G.711 is used, it is vulnerable to the bug since it is not perfectly divisible by 8000.</p> <p>Workaround: Specify the minimum reserved rate to be a multiple of 8000.</p>
CSCsb63551	<p>When examining the local CMTS uBR100012, the router log the following messages:</p> <pre data-bbox="613 888 894 909">%AMDP2_FE-6-EXCESSCOLL</pre> <p>This issue can occur under normal operating conditions and with light load. This fix will correct these errors.</p> <p>There are no known workarounds.</p>
CSCsb69505	<p>If the previous streaming/export process is incomplete (data-incomplete), then for the current export, the XML file shows wrong IPDRDoc.End count= value.</p> <p>There are no known workarounds.</p>
CSCsb71967	<p>After the reboot, the config on the specific upstreams have changed from 3200000 to 1600000 in 2 specific upstreams.</p> <p>This issue is seen in cable-mc16c cards in 12.3(13a)BC when spectrum-group is configured (not seen in 12.3(9a)BC).</p> <p>Workaround: Configure 3200000 manually in the affected upstreams manually after reboot.</p>
CSCsb74136	<p>An unexpected reload will occur when using old Flash Memory and old-style PCMCIA cards like slot0: and slot1: with a small value for the <b>cable sflog</b> command.</p> <p>It is advised that, while using SAMIS, to use newer ATA style PCMCIA cards. Also, the recommended value for the <b>sflog</b> command is as below to obtain deleted service flows. If other values are used, sflog file might need to be created in the filesystem and with slot0: and slot1: being used for the sflog file, the unexpected reload might occur:</p> <pre data-bbox="613 1665 1224 1686">cable sflog max-entry 40000 entry-duration 86400</pre> <p>Workarounds: Use <b>cable sflog max-entry 40000 entry-duration 86400</b> to collect the deleted service flow information in SAMIS.</p> <p>Alternative workaround: Use newer ATA style flash cards like disk0:, disk1:</p>

Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCsb74236	<p>When changing modem configuration from 1.0 to 1.1, the docsQosServiceFlowTimeCreated does not updated with new time. It shows previous Time(1.0 SF creation Time).</p> <p>Workaround: Perform the following:</p> <ul style="list-style-type: none"> <li>• Up the modem with 1.0 configuration.</li> <li>• Change the configuration file with 1.1.</li> <li>• Reset the modem for taking the 1.1 configuration.</li> </ul>
CSCsb76288	<p>The <b>card</b> configuration command is not always propagated to the standby Performance Routing Engine (PRE) if OIR-compatibility is enabled. This results in a configuration mismatch between the standby and active PREs where the card is present in the running configuration of the active PRE but not in the standby PRE.</p> <p>This issue occurs when the OIR-compatibility is enabled on the slot, and the <b>card</b> command is specified an MC520 type line card.</p> <p>Workaround: Re-issue the <b>no card slot/subslot</b> command followed by the <b>card slot/subslot cardtype</b> command.</p>
CSCsb76299	<p>A given service class when added to admission control configuration, may not take effect.</p> <p>This issue occurs if the name of the service class is exactly 15 characters long.</p> <p>Workaround: Make the service class name shorter than 15 characters.</p>
CSCsb76409	<p>A cable modem provisioned for DOCSIS 1.1 or greater can bypass BPI+ and register using BPI by not providing a CM certificate in its Authorization Request. This allows hackers to bypass the additional security features provided by BPI+. By establishing BPI privacy, the hacker is also able to avoid the “cable privacy mandatory” setting available on CMTS interfaces.</p> <p>This issue only occurs when a non DOCSIS compliant CM sends such an auth-request message, and the only known modems to do so are miscreant cable modems.</p> <p>There are no known workarounds.</p>
CSCsb76667	<p>GE link flap with Transparent LAN Service (TLS) after N+1 switchover, so end-to-end TLS traffic fail for a few seconds.</p> <p>This issue occurs on Cisco IOS Releases 12.3(9a)BC6 and 12.3(13a)BC and configured TLS and N+1 environment.</p> <p>There are no known workarounds.</p>
CSCsb77154	<p>Packets that do not match any criteria in a filter group are dropped on a Cisco uBR10000 series router.</p> <p>This issue only occurs on a Cisco uBR10000 series router.</p> <p>Workaround: Manually create an entry in the packet filter group that will accept all packets. This entry should be the last one in the packet filter group.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCsb85033	<p>If secondary RKS does not exist, configure a bogus Secondary RKS IPAddr in CMS, don't send it NULL (0.0.0.0).</p> <p>There are no known workarounds.</p>
CSCsb86672	<p>Cable modems are online but the MTA is not getting IPs.</p> <p>Workaround: Microcode reload pxf.</p>
CSCsb96390	<p>When utilizing Cisco IOS Release 12.3(13a)BC on a Cisco uBR10012 CMTS configured for N+1 redundancy, MPLS, and PacketCable calls switchover scenarios can cause calls to drop and also modems to go offline when they should remain online.</p> <p>This issue occurs on an Cisco uBR10012 running RF line card redundancy with MPLS and PacketCable configured. Initiate RF line card switchovers with OIR, test crash, or CLI.</p> <p>There are no known workarounds.</p>
CSCsb99726	<p>The Cisco router may not be able to utilize the full DS bandwidth on a 520 line card.</p> <p>This issue occurs when multiple BE service flows try to utilize the full DS bandwidth on a 520 line card.</p> <p>There are no known workarounds.</p>
CSCsc00363	<p>Traceback occur repeatedly on PRE2.</p> <pre data-bbox="613 1066 1507 1213"> Sep 26 13:47:20.547: %GENERAL-3-EREVENT: No current_if_info for hwidb Cable7/0/0 icb 114688: subint 0 dlci_or_handle 1 &lt;---Traceback---&gt; Sep 26 13:47:25.947: %GENERAL-3-EREVENT: No current_if_info for hwidb Cable6/1/1 icb 106752: subint 0 dlci_or_handle 1 &lt;---Traceback---&gt; </pre> <p>This issue occurs in Cisco IOS Release 12.3(9a)BC7 with PRE2 using multicast function.</p> <p>There are no known workarounds.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description																
CSCsc02003	<p>Unable to ping from Cisco uBR10000 (PRE2) to anything (DHCP server, modem, PC, etc.), and uBR10000 cannot forward any IP packet (except FastEthernet).                      PXF also appears to be stuck:</p> <p>Output of "show pxf dma" indicates the following errors.                      From RP Counters:                          Packets: 148, Cumulative Bytes: 12358                          Output Drops: 0, Own Errors 22961, FromRP Interrupts 279309                          PXF DMA New Work TTQ Full Error: 3258                          PXF DMA FBTTQ Full Error: 3314</p> <p>Output of "show pxf cpu context" indicates high cpu utilization.</p> <table border="1" data-bbox="586 625 1312 751"> <thead> <tr> <th>FP context utilization</th> <th>1min</th> <th>5min</th> <th>60min</th> </tr> </thead> <tbody> <tr> <td>Actual</td> <td>99 %</td> <td>99 %</td> <td>94 %</td> </tr> <tr> <td>Theoretical</td> <td>98 %</td> <td>98 %</td> <td>55 %</td> </tr> <tr> <td>Maximum</td> <td>98 %</td> <td>98 %</td> <td>58 %</td> </tr> </tbody> </table> <p>This issue occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>- On Cisco IOS Release 12.3(9a)BC7 or 12.3(13a)BC with PRE2</li> <li>- On a PBR setting on cable interface</li> <li>- On a service-policy (LLQ) setting on Gigabit Ethernet interface</li> <li>- When pinging from PC to PC under CM during several minutes</li> </ul> <p>Workaround: Reload the router. However, this is a temporary workaround as the issue reproduces after reloading too.</p>	FP context utilization	1min	5min	60min	Actual	99 %	99 %	94 %	Theoretical	98 %	98 %	55 %	Maximum	98 %	98 %	58 %
FP context utilization	1min	5min	60min														
Actual	99 %	99 %	94 %														
Theoretical	98 %	98 %	55 %														
Maximum	98 %	98 %	58 %														
CSCsc02416	<p>A Cisco uBRk10000 series router running Cisco IOS Release 12.3(9a)BC6 experiences the following bus error:</p> <p>System returned to ROM by bus error at PC 0x602BF6E4, address 0x4824                      This issue occurs on a Cisco uBR10000 series router running a PRE1 with MC28c &amp; MC520u cards and 15,000 attached devices.</p> <p>Workaround: Do not use the <b>cable modem mac- addr access-group access group number</b> command on the Cisco uBR10000 series router. This command is not supported on the Cisco uBR10000 series router.</p>																
CSCsc06630	<p>Executing the <b>hw-module subslot slot/subslot reset</b> command generates non-blocking request and destination port tracebacks:</p> <pre>*Oct 4 12:17:56.784: %REQGRP-3-SYSCALL: System call for command 6 (slot8/0) : Nonblocking request failed (Cause: timeout) -Traceback= 60378C84 606BFC84 606C226C 606C290C 606C3100 *Oct 4 12:18:02.368: %IPC-5-INVALID: Invalid dest port=0x0 -Traceback= 606C0508 606CC39C 606CC22C 606CC4A0 6067BBCC 6067C0D8 6067C59C</pre> <p>This issue occurs when the user resets a line card using either the <b>hw-module subslot reset</b> or <b>hw-module slot reset</b> command.</p> <p>There are no known workarounds.</p>																

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

DDTS ID Number	Description
CSCsc07695	<p>Unable to ping PC-to-PC under cable modem with TLS setting.</p> <p>This issue is seen on Cisco IOS Release 12.3(9a)BC7 with TLS setting and occurs if the TLS setting is read from startup-config. However, there is no problem when setting it after booting.</p> <p>Workaround: Reset the <b>cable dot1q-vc-map</b> command.</p>
CSCsc08300	<p>If a Hot Standby Connection-to-Connection Protocol (HCCP) switchover occurs due to an unexpected reload or OIR, when the Working LC comes back into service; an auto-revert will occur (instead of waiting for the revert time to expire).</p> <p>Workaround: For the OIR case, issue a CLI switchover first. For the unexpected reload case, there are no known workarounds.</p>
CSCsc09378	<p>When changing the host name in CMTS, SAMIS XML record replaces the previous hostname with new hostname in the tag CMTShostname.</p> <p>Workaround: Change the hostname in CMTS and do the metering.</p>
CSCsc11996	<p>A problem in the CMTS codebase may cause Cisco uBR10000 series routers to unexpectedly reload due to a memory corruption.</p> <p>This unexpected reload occurs in configurations using both IGMP and BPI+ when the number of multicast addresses assigned to a single multicast SID exceeds 119. The code supports a maximum of 8 multicast addresses per multicast SID per modem.</p> <p>Workaround: Use ip access lists to organize the multicast addresses into groups of eight. Then use the <b>cable match address</b> interface configuration command to create a multicast SAID for each group of addresses.</p>
CSCsc12259	<p>On a Cisco uBR10000 CMTS, if the cable source-verify feature is active then the “no buffer” counter in the output of the <b>show interface cable if-number</b> command may go backwards or even become negative.</p> <p>The cable source-verify feature must be active and engaged in dropping packets for this issue to occur.</p> <p>There are no known workarounds. However the problem is cosmetic and will not impact on normal router operations.</p>
CSCsc14981	<p>There will be missing “docsQosCmtsIfIndex” entries if CLC OIR to different slot on the CMTS. When we query the MIB object, it will return nothing.</p> <p>This issue occurs if the customer uses the default value for the CLI command <b>cable cmcpe valid-time 900</b>. If there is no such configuration, most likely it is using the default 900sec value.</p> <p>Workaround: Use the CLI command <b>cable cmcpe valid-time 0</b>.</p>
CSCsc16554	<p>IGMP state limit counters increase (upon join) but do not decrease (upon leave) resulting in denial.</p> <p>This issue only occurs when SSM is combined with IGMP state limit (which then requires source mapping).</p> <p>There are no known workarounds.</p>

**Table 78**      **Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsc20781	<p>There will be a missing MIB entry (docsQosServiceFlowPrimary) with VIB config.</p> <p>Workaround: Do not configured VIB.</p>
CSCsc33027	<p>Average upstream channel utilization counter will not update after line card switchover. Despite no traffic going to the card, the percent utilization still remains high.</p> <p>There are no known workarounds.</p>
CSCsc33766	<p>Modems fail to come online and reach init(d) state.</p> <p>An OIR of MC520 (S/U/T) where there is a change in card type (S/U/T), and the interfaces on the line card are Virtual Bundle members, will result in modems failing DHCP.</p> <p>Workaround: A shut/no shut of the affected Cable interfaces will allow the modems to come online.</p> <p>Alternative workaround: Remove the affected interfaces from the Bundle and add back to the bundle.</p>
CSCsc35263	<p>With Global HA configured, shutting down all interfaces on C6/1 or C8/0 causes failover of Cx/y/1 through Cx/y/4, and no failover on Cx/y/0.</p> <p>There are no known workarounds.</p>
CSCsc35974	<p>Multicast packets was not able to be forwarded to cable interface, irrespective of whether using DSG is being used or not. Due to this reason, Host and POD in set-top box (STB) were not able to get ip address from DHCP server, and eCM in STB is operating DOCSIS.</p> <p>There are no known workarounds.</p>
CSCsc37564	<p>Cable intercept might not send copy of Downstream packets to the collection server. Only Upstream packets appear on the collection server.</p> <p>There are no known workarounds.</p>
CSCsc39508	<p>The IGMP command <b>ip igmp static-group *</b> does not function.</p> <p>Workaround: All static groups have to be added manually (one at a time).</p>
CSCsc42019	<p>When configuring N+1 global with Virtual Interface Bundling, the Hot Standby Connection-to-Connection Protocol (HCCP) never goes into the ready state due to the following error:</p> <pre>Static Sync is running, wait for another 1 min, renew hccp suspend timer</pre> <p>HCCP keeps restarting its counters.</p> <p>There are no known workarounds.</p>
CSCsc44370	<p>LC switchovers corrupts CM state, which includes CM replication in the database, and ends up in weird state.</p> <p>There are no known workarounds.</p>

**Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsc44856	<p>After Hot Standby Connection-to-Connection Protocol (HCCP) switchover, CEF may have adjfibs in the wrong VRF and incomplete adjacencies.</p> <p>This issue occurs on a Cisco uBR10000 with cable modem interface redundancy switching over from a subinterface in one VRF to an interface in a different VRF.</p> <p>There are no known workarounds.</p>
CSCsc46991	<p>User cannot change service policy. Attempting to change service-policy.</p> <p>There are no known workarounds.</p>
CSCsc48502	<p>The OIR-compatibility feature fails to restore shared upstream connector settings when exchanging compatible cable line cards (i.e. 520U to 520S).</p> <p>This issue occurs on an OIR of MC520 (S/U/T) where there is a change in card type (S/U/T), and one or more interfaces on the line card are configured to share upstream connectors.</p> <p>Workaround: Manually restore the configuration.</p>
CSCsc51925	<p>Test bed unexpectedly reloads.</p> <p>This issue started after inserting an HFC distance into the plant for C5/0/0 up 2 and up 3, and also adding a uBR924 cable modem to the same port. uBR924 cable modem cannot obtain an IP address. (Ref CSCeh48461).</p> <p>There are no known workarounds.</p>
CSCsc55518	<p>PRE2 unexpectedly reloads with the following error in the reload info:</p> <p style="text-align: center;">PXF DMA Error - End of Descriptor Before Cmd Byte Length Exhausted</p> <p>There are no known workarounds.</p>
CSCsc58373	<p>CISCO CMTS is needed to send random MPEG NULL frames. Certain chipset cable modems might not get a lock at DS 256QAM signal.</p> <p>There are no known workarounds.</p>
CSCsc62224	<p>A CMTS Running 12.3(13a)BC code will report a value of “unknown (4)” in the ifOperStatus and ifAdminStatus of Cable subinterfaces when queried by SNMP.</p> <p>This issue occurs when querying the ifTable of any CMTS which is configured with Cable subinterfaces. This affects any CMTS running 12.3(13a)BC code.</p> <p>There are no known workarounds.</p>
CSCsc64567	<p>While conducting an OIR on subslot 8/0, CMTS attempted a failover to the Protect, 5/1 while 5/1 was active and already protecting 8/1. The result was that all the modems on 5/1 went offline and then back online.</p> <p>There are no known workarounds.</p>
CSCsc64649	<p>Under heavy congestion, downstream packets may be dropped on 520 cable line cards. The packets may be dropped without regard to priority.</p> <p>There are no known workarounds.</p>

Table 78 Resolved Caveats for Cisco IOS Release 12.3(17a)BC (continued)

DDTS ID Number	Description
CSCsc66344	<p>With Bundle interfaces and SSM configured using “ip igmp static-group 232.1.1.1 source 4.22.2.3” on the bundle and a second source for 232.1.1.1 using DNS, the only source to pass is the DNS defined source. Both should pass with priority to the static-group command on the bundle.</p> <p>There are no known workarounds.</p>
CSCsc68382	<p>The following error message may appear in the log of a Cisco UBR1000:</p> <pre>%GENERAL-3-EREVENT: No current_if_info for hwidb Cable6/0/2 icb 98816: subint 1 dlci_or_handle 512 -Traceback= 600F6504 600DF07C 600E5F3C 600E6040 600E72A4 600E748C 60D5ECDC 60D5DF34 60D5F708 60406548 60D62A78 60408864 60408BE0 605718D0 605718B4</pre> <p>This error occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>- MPLS/VPN route leaking is configured</li> <li>- A cable interface belongs to a vrf with route-leaking</li> <li>- When the customer premises equipment (CPE) is behind a cable modem that is hanging of the above-mentioned cable interface gets an IP address through DHCP, the traceback is shown.</li> </ul> <p>There are no known workarounds.</p>
CSCsc77315	<p>On a Cisco uBR10000 series CMTS, after a Cable Line Card switchover event occurs, the list of cable modems listening to a particular BPI+ encrypted multicast stream may be truncated to only the first modem to join the stream.</p> <p>The cable modem list may be seen with the command <b>show interface cable interface-number sid mcast-sid</b>.</p> <p>This issue occurs after a cable line card failover on a CMTS that has Cable Line Card redundancy enabled.</p> <p>There are no known workarounds. However, this issue does not affect encrypted multicast streams being received by cable modems.</p>
CSCsd06576	<p>If <b>boot config config_file_name</b> is shown or is configured in the running-config, startup-config on the standby nvram is deleted. Even issuing <b>write mem</b> does not recreate the file, so when the standby becomes active, all configuration gets wiped out.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(13a)BC6

Table 79 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC6.

**Table 79** Open Caveats for Cisco IOS Release 12.3(13a)BC6

DDTS ID Number	Description
CSCeh89315	<p>The counters for leasequery-filter do not get cleared when <b>clear counters</b> or <b>clear counters cablex/y</b> is issued after the leasequery-filter related CLI has been un-configured.</p> <p>Workaround: Clear the counters while the CLI is in effect and then un-configure it.</p>
CSCei22859	<p>The secondary service does not pass traffic after a line card switchover.</p> <p>This issue is likely related to payload header suppression (PHS) traffic and switchovers.</p> <p>Workaround: Do not use PHS.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are being forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCei54145	<p>After a quality of service (QoS) enforcement and modem reset, the modem takes the recently created profile and not the QoS profile that was in use before modem reset.</p> <p>There are no known workarounds.</p>
CSCei54281	<p>With N+1 switchovers, the number of expected customer premises equipment (CPE) devices does not get reflected in the <b>show cable modem verbose</b> command.</p> <p>This issue occurs in a Performance Routing Engine High Availability (HA) configuration.</p> <p>There are no known workarounds.</p>
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>

Table 79 Open Caveats for Cisco IOS Release 12.3(13a)BC6 (continued)

DDTS ID Number	Description
CSCek37177	<p>The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.</p> <p>This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.</p> <p>Cisco has made free software available to address this vulnerability for affected customers.</p> <p>This issue is documented as Cisco bug ID <a href="#">CSCek37177</a>.</p> <p>There are workarounds available to mitigate the effects of the vulnerability.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-tcp">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-crafted-tcp</a></p>
CSCin95131	<p>The Protected interface's modem entries are not in the docsIfCmtsMacToCmTable after multiple RPR/N+1 switchovers.</p> <p>There are no known workarounds.</p>
CSCsb02318	<p>The following Hot Standby Connection-to-Connection Protocol (HCCP) configuration commands may not preserve their non-default configuration values after two Performance Routing Engine (PRE) switchovers unless the running-config is saved to startup-config before PRE switchover.</p> <pre>[no] hccp x authentication [no] hccp x revertive [no] hccp x reverttime [no] hccp x timers [no] hccp x track       (here x: groupnumber )</pre> <p>For example, assume that PRE-A is the active PRE and that PRE-B is the standby PRE. When a switchover from PRE-A to PRE-B happens, PRE-A will be reset and rebooted. After rebooting, during the configuration, PRE-B will send its running-config over to PRE-A. This running-config will become PRE-A's startup-config. PRE-A will try to parse this configuration and start applying it. If the running-configuration on PRE-A was not saved before switchover, the user configured values of these commands will be absent.</p> <p>Workaround: Save the running-config to startup-config whenever the above commands are issued.</p>
CSCsb14936	<p>SNMPv3 gets/sets fail following a Performance Routing Engine (PRE) switchover and attempts to increment usmStatsWrongDigests.0.</p> <p>This issue exists in a configuration with Route Processor Redundancy (plus) (RPR+) that uses SNMPv3, where the SNMP EngineID value is the default value.</p> <p>Workaround: Specify a value for the SNMP EngineID using the global configuration <b>snmp-server engineID local</b> <i>[octet-string]</i> command, where <i>octet-string</i> is the desired engineID value.</p>

**Table 79**      **Open Caveats for Cisco IOS Release 12.3(13a)BC6 (continued)**

DDTS ID Number	Description
CSCsb17060	<p>The default profiles 21/41 and 121/141 appear in the <b>show running-config</b> command even if the user configures them with same values as the defaults in the <b>cable modulation-profile</b> commands.</p> <p>Workaround: Avoid using the <b>cable modulation-profile</b> command unless you need to explicitly indicate a non-default modulation profile.</p>
CSCsb20032	<p>After the <b>shut</b> of an interface and then removal of legacy High Availability (HA) commands from the <b>shut</b> interface, a Performance Routing Engine (PRE) failover was performed from PREA to PREB. After the PRE switchover, the corresponding Protect interface is now in the *ACTIVE* state.</p> <p>There are no known workarounds.</p>
CSCsb29527	<p>A Cisco uBR10000 series cable modem termination system (CMTS) ca not provide the full minimum reserved rate configured for a downstream service flow.</p> <p>The issue occurs when the downstream channel of the cable interface that the modem is connected to is experiencing congestion.</p> <p>There are no known workarounds.</p>
CSCsb30593	<p>When there are more than 10 downstream packet classifiers per-modem, the packet classifiers do not count matching packets.</p> <p>This issue only occurs when there are more than 10 packet classifiers on a single modem, a very rare configuration.</p> <p>There are no known workarounds.</p>
CSCsb37557	<p>The term “SNR” in the <b>show cable modem phy</b> and <b>show controller</b> commands is confused with “CNR” by customers.</p> <p>This issue occurs when running the <b>show cable modem phy</b> and <b>show controller</b> commands.</p> <p>There are no known workarounds.</p>
CSCsb40202	<p>The current implementation of cable filter groups can allow a cable modem or a customer premises equipment (CPE) device to bypass filters.</p> <p>There are two cases where this issue can be triggered:</p> <ol style="list-style-type: none"> <li data-bbox="621 1402 1520 1518">1. MSO configures the cable modem termination system (CMTS) with default cable filter groups with the <b>cable submgmt default filter-group</b> command and points them to a group ID that does not exist. IOS will not give a warning, and the device is completely open.</li> <li data-bbox="621 1539 1520 1633">2. Data-over-Cable Service Interface Specification (DOCSIS) 1.1 provisioned cable modems have TLV 37 configured, but point to a group ID that does not exist. IOS gives no warning, and the device is completely open.</li> </ol> <p>In cases where a group ID does not exist, the default behavior of IOS should probably be a “deny all” like traditional ACLs instead of the current “permit all”.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(13a)BC6

Table 80 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC6.

**Table 80** Resolved Caveats for Cisco IOS Release 12.3(13a)BC6

DDTS ID Number	Description
CSCeh48889	<p>The INVALIDSIDPOSITION message occurs on an interface when a large number of cable modems are going online and offline at once</p> <p>For example:</p> <pre>%UBR10000-3-INVALIDSIDPOSITION: Invalid SID (4184) position for interface Cable5/0/0: CM 00d1.1477.7451:Is used by CM 00d0.d726.ef0b SFID 6813 SID 4184. SID container info: start 744 end 6967 -Traceback= 6030A628 6030A844 6030B098 602F81FC 603A480C 605E1398 605E137C</pre> <p>One typical trigger for this message is the <b>clear cable modem delete</b> or <b>clear cable modem oui oui delete</b> command. The affected modem is kicked offline and will usually come back online later. Many different modems may be affected.</p> <p>Workaround: <b>Shut /no shut</b> the affected cable interface, or delete most modems on the cable interface.</p> <p>Alternative workaround: Reduce the number of cable modems on the affected cable interface by moving modems to other ports.</p>
CSCek36686	<p>A PRE2 card unexpectedly reloads if a cable intercept configuration is added/removed for a cable modem which is transitioning between different Data-over-Cable Service Interface Specification (DOCSIS) states.</p> <p>This issue occurs when the debug cable intercept command is used.</p> <p>Workaround:</p> <ol style="list-style-type: none"> <li>1. Do not remove/adda cable intercept related configuration for a cable modem from the cable modem termination system (CMTS) while that cable modem is in a transitioning state.</li> <li>2. Do not turn on any cable intercept debugs on CMTS.</li> </ol>
CSCek39658	<p>The value of CMTipAddress in the IP Detail Record (IPDR) information, sent by the cable modem termination system (CMTS) when cable billing is configured is currently set to the lowest IP address numerical value on the CMTS. This value is not guaranteed to be consistent for a given CMTS.</p> <p>There are no known workarounds.</p>
CSCek50191	<p>When configuring a cable monitor with the ACL option, the cable modem termination system (CMTS) flushes out traceback and spurious memory access.</p> <p>There are no known workarounds.</p>

**Table 80 Resolved Caveats for Cisco IOS Release 12.3(13a)BC6 (continued)**

DDTS ID Number	Description
CSCin92949	<p>When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.</p> <p>This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.</p> <p>Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.</p>
CSCsa69446	<p>Authentication, Authorization, and Accounting (AAA) authorization does not work with login authentication configured for line, nor with if- authenticated keyword.</p> <p>Workaround: Use either "enable" or "Local" as the fallback authentication method.</p>
CSCsc43642	<p>A cable modem termination system (CMTS) can experience an intermittent problem with cable modems being able to pass traffic, but not being pingable. The cable modems stay online and the customer premises equipment (CPE) behind the cable modem are pingable.</p> <p>Only cable modems are affected; the CPE IP addresses are correct.</p> <p>The following is an example of this issue:</p> <pre>Router# show cable modem a.b.c.d MAC Address      IP Address      I/F      MAC      Prim RxPwr Timing  Num BPI Offset  CPE Enb xxx.yyy.zzz  a.b.c.d      C7/0/3/U0 online      2839 -3.00 2262  1  N Router# show controllers cable 7/0/3 u 0   i SNR   US phy SNR_estimate for good packets - 27.1419 dB</pre> <p>The issue is most prevalent on Cisco uBR10000 series routers.</p> <p>Workaround: Reset the modem(s) through the CLI or power cycle. The issue can sometimes disappear by itself; pinging the CPE also helps.</p>
CSCsd31933	<p>If many modems are not registered at the cable modem termination system (CMTS) and logging is enabled at the CMTS console, a route processor can crash due to high CPU utilization.</p> <p>This symptom occurs on a Cisco uBR10000 series router.</p> <p>Workaround: Avoid enabling the logging console message at CMTS console if many modems are not registered.</p>
CSCsd67203	<p>The Cable Metering process stalls on a Cisco uBR10000 series router running Cisco IOS Release 12.3(13a)BC2.</p> <p>This condition causes a memory leak, which eventually requires the cable modem termination system (CMTS) to be reloaded when the <b>cable sflog</b> command is configured. Messages such as:%% Low on memory; try again later appear when accessing the box, issuing <b>show</b> commands, or configuring the CMTS.</p> <p>Workarounds: 1. Remove the <b>cable sflog</b> command. 2. Failover the Performance Routing Engine (PRE), and reload the CMTS to free memory.</p>

**Table 80 Resolved Caveats for Cisco IOS Release 12.3(13a)BC6 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsd90835	<p>High downstream (DS) latency occurs on the MC520.</p> <p>The primary symptoms include excessive ping times (up to 1000 milliseconds), and spurious memory access.</p> <p>There are no known workarounds.</p>
CSCsd97968	Support for additional error checking was added to the code.
CSCse00016	<p>The PXF_Crashinfo file write operation fails to complete.</p> <p>This issue may occur due to an unscheduled restart of parallel express forwarding (PXF).</p> <p>There are no known workarounds.</p>
CSCse00861	<p>On a Cisco uBR10000 series router the cable modem termination system (CMTS), cable modems and connected customer premises equipment (CPE) are not able to be pinged after a Hot Standby Connection-to-Connection Protocol (HCCP) line card failover to a Protect line card.</p> <p>This issue can affect cable modems if they are using BPI encryption and connected to the second upstream channel to be sharing an upstream connector using the frequency stacking functionality.</p> <p>Workaround: Disable BPI encryption and/or not use frequency stacking, or connector sharing, when HCCP switchovers may occur. Affected cable modems and CPE will become pingable again after the failed over MAC domain is reverted back from the Protect line card to the Working line card. Affected cable modems may also regain IP connectivity after being reset.</p>
CSCse24179	<p>The dynamic service flow created for PacketCable Multimedia (PCMM) sessions for the Speed Preview application hang.</p> <p>Workaround: Because the Speed Preview application cannot set the PCMM T3 timer (DOCSIS T8 timer), the only way to clean up the service flow is to identify the flows that are stuck and enter <b>test cable dsd ip-addr-of-modem</b> command.</p>
CSCse25429	<p>While netbooting the cable modem termination system (CMTS) with the latest geo_cable image, the CMTS crashes.</p> <p>This issue occurs when CMTS has unsupported DSG1.2 configurations on the startup at the time of netbooting.</p> <p>Workaround: Load the image without having any unsupported DSG configurations on the startup.</p>
CSCse28069	<p>High CPU usage in the TTY background occurs on a terminal server connected to a Cisco uBR10000 series router (PRE2) when the <b>modem inout</b> command is configured.</p> <p>Workaround: Disable the <b>modem inout</b> command.</p>
CSCse50424	<p>On a Cisco uBR10000 series router, PRE2 is experiencing high CPU usage and crashes when querying the customer premises equipment (CPE) (40 CPEs) by the Simple Network Management Protocol (SNMP).</p> <p>There are no known workarounds.</p>

**Table 80 Resolved Caveats for Cisco IOS Release 12.3(13a)BC6 (continued)**

DDTS ID Number	Description
CSCsb19763	<p>CF flash cannot be read between redundant eRSC cards.</p> <p>This condition occurs when a CF flash card is formatted in one eRSC slot and the IOS and firmware are TFTP'd to the CF flash card. If the formatted flash card is removed and inserted into a different eRSC slot, the newer RSC slot cannot read the CF.</p> <p>Workaround: Associate a CF flash card to a particular eRSC and keep it with that card. TFTP all need files to the CF either using the LAN or local TFTP laptop.</p>
CSCse04195	<p>PRE2 resets due to a PXF DMA Error - Input Command Has Sequence Problem.</p> <p>There are no known workarounds.</p>
CSCse04266	<p>A Cisco uBR10000 series router reset occurs at sch_rp_first_mac_rw_in_chain.</p> <p>This condition occurs on a Cisco uBR10000 series router with PRE2.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(13a)BC5

Table 81 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC5.

**Table 81 Open Caveats for Cisco IOS Release 12.3(13a)BC5**

DDTS ID Number	Description
CSCeh89315	<p>The counters for leasequery-filter do not get cleared when <b>clear counters</b> or <b>clear counters cablex/y</b> is issued after the leasequery-filter related CLI have been unconfigured.</p> <p>There are no known workarounds.</p>
CSCei22859	<p>The secondary service does not pass traffic after a line card switchover.</p> <p>This issue is likely related to payload header suppression (PHS) traffic and switchovers.</p> <p>Workaround: Do not use PHS.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are being forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCei54145	<p>After Qos enforcement and modem reset, the modem takes the recently created profile and not the qos profile that was in use before modem reset.</p> <p>There are no known workarounds.</p>
CSCei54281	<p>With N+1 switchovers, the number of expected customer premises equipment (CPE) devices does not get reflected in the <b>show cable modem verbose</b> command.</p> <p>This issue occurs in a Performance Routing Engine High Availability (HA) configuration.</p> <p>There are no known workarounds.</p>

Table 81 Open Caveats for Cisco IOS Release 12.3(13a)BC5 (continued)

DDTS ID Number	Description
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>
CSCin92949	<p>When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.</p> <p>This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.</p> <p>Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.</p>
CSCin95131	<p>Protector interface's modem entries would not be there in the docsIfCmtsMacToCmTable after multiple RPR/N+1 switchovers.</p> <p>There are no known workarounds.</p>
CSCsb02318	<p>The following Hot Standby Connection-to-Connection Protocol (HCCP) configuration commands may not preserve their non-default configuration values after two Performance Routing Engine (PRE) switchovers unless the running-config is saved to startup-config before PRE switchover.</p> <pre>[no] hccp x authentication [no] hccp x revertive [no] hccp x reverttime [no] hccp x timers [no] hccp x track       (here x: groupnumber )</pre> <p>Assume that PRE-A is the active PRE and PRE-B is the standby PRE. When a switchover from PRE-A to PRE-B happens, PRE-A will be reset and rebooted. After rebooting, during the configuration, PRE-B will send its running-config over to PRE-A. This running-config will become PRE-A's startup-config. PRE-A will try to parse this configuration and start applying it. If the running-configuration on PRE-A was not saved before switchover, the user configured values of these commands will be absent.</p> <p>Workaround: Save the running-config to startup-config whenever the above commands are issued. This restriction will be relaxed in the next release.</p>
CSCsb14936	<p>SNMPv3 gets/sets fail following Performance Routing Engine (PRE) switchover. Attempts increment usmStatsWrongDigests.0.</p> <p>This issue exists in a configuration with RPR+ and that uses SNMPv3, where the snmp EngineID value is the default value.</p> <p>Workaround: Specify a value for the snmp EngineID via the global configuration CLI: <b>snmp-server engineID local</b> [octet string] where octet string is the desired engineID value.</p>

**Table 81**      **Open Caveats for Cisco IOS Release 12.3(13a)BC5 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb17060	<p>The default cable modulation profile does not appear within the <b>show running-config</b> command even though the <b>cable modulation-profile</b> command is apparently configured.</p> <p>Workaround One: Configure the <b>cable modulation-profile initial</b> command.</p> <p>Workaround Two: Configure the <b>cable modulation-profile</b> command with no values.</p>
CSCsb20032	<p>After <b>shut</b> of an interface and then removal of legacy HA commands from the <b>shut</b> interface, a Performance Routing Engine (PRE) failover was performed from PREA --&gt; PREB. It was observed that after a PRE switchover, the corresponding PROTECT interface is now in *ACTIVE* state.</p> <p>There are no known workarounds.</p>
CSCsb26657	<p>The toaster feed_back context rate is excessive when multicast traffic is present.</p> <p>There are no known workarounds.</p>
CSCsb29527	<p>A Cisco uBR10000 series CMTS may not provide the full Minimum reserved rate configured for a downstream service flow.</p> <p>The issue may occur when the downstream channel of the cable interface that the modem is connected to is experiencing congestion.</p> <p>There are no known workarounds.</p>
CSCsb30593	<p>Per-modem downstream packet classifiers greater then 10 do not count matching packets.</p> <p>This issue only occurs when there are more than 10 packet classifiers on a single modem, a very rare configuration.</p> <p>There are no known workarounds.</p>
CSCsb37557	<p>The term SNR in <b>show cable modem phy</b> and <b>show controller</b> is easily confused with CNR by customers.</p> <p>This issue occurs when running command <b>show cable modem phy</b> and <b>show controller</b>.</p> <p>There are no known workarounds.</p>
CSCsb40202	<p>The current implementation of cable filter groups can allow a CM or customer premises equipment (CPE) device to bypass filters.</p> <p>There are two cases where this issue can be triggered:</p> <ol style="list-style-type: none"> <li>1. MSO configures the CMTS with default cable filter groups with the <b>cable submgmt default filter-group</b> command and points them to a group ID that does not exist. IOS will not give a warning, and the device is completely open.</li> <li>2. DOCSIS1.1 provisioned CMs have TLV 37 configured, but points to a group ID that does not exist. IOS gives no warning, and the device is completely open.</li> </ol> <p>In cases where a group ID does not exist, default behavior of IOS should probably be a “deny all” like traditional ACLs instead of the current “permit all”.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(13a)BC5

Table 82 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC5.

**Table 82** Resolved Caveats for Cisco IOS Release 12.3(13a)BC5

DDTS ID Number	Description
CSCsd81136	<p>After a line card switchover, one or more cable modems (CMs) are stuck in the init(i) state.</p> <p>This issue may occur if the CMs are provisioned with privacy and was observed in a DOCSIS 1.1 environment after a switch over (Working to Protect) and subsequent switch back (Protect to Working).</p> <p>Workaround: To clear up a single modem in this state,try entering the following commands:</p> <pre>clear cable modem h.h.h delete clear ip arp d.d.d.d</pre> <p>where <i>h.h.h</i> is the mac-address of the stuck CM and <i>d.d.d.d</i> is the IP address of that same CM.</p>

## Open Caveats for Release 12.3(13a)BC4

Table 83 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC4.

**Table 83** Open Caveats for Cisco IOS Release 12.3(13a)BC4

DDTS ID Number	Description
CSCeh89315	<p>The counters for leasequery-filter do not get cleared when <b>clear counters</b> or <b>clear counters cablex/y</b> is issued after the leasequery-filter related CLI have been unconfigured.</p> <p>There are no known workarounds.</p>
CSCei22859	<p>The secondary service does not pass traffic after a line card switchover.</p> <p>This issue is likely related to payload header suppression (PHS) traffic and switchovers.</p> <p>Workaround: Do not use PHS.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are being forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCei54145	<p>After Qos enforcement and modem reset, the modem takes the recently created profile and not the qos profile that was in use before modem reset.</p> <p>There are no known workarounds.</p>

**Table 83**      **Open Caveats for Cisco IOS Release 12.3(13a)BC4 (continued)**

DDTS ID Number	Description
CSCei54281	<p>With N+1 switchovers, the number of expected customer premises equipment (CPE) devices does not get reflected in the <b>show cable modem verbose</b> command.</p> <p>This issue occurs in a Performance Routing Engine High Availability (HA) configuration.</p> <p>There are no known workarounds.</p>
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>
CSCin92949	<p>When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.</p> <p>This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.</p> <p>Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.</p>
CSCin95131	<p>Protector interface's modem entries would not be there in the docsIfCmtsMacToCmTable after multiple RPR/N+1 switchovers.</p> <p>There are no known workarounds.</p>
CSCsb02318	<p>The following Hot Standby Connection-to-Connection Protocol (HCCP) configuration commands may not preserve their non-default configuration values after two Performance Routing Engine (PRE) switchovers unless the running-config is saved to startup-config before PRE switchover.</p> <pre data-bbox="656 1266 987 1423"> [no] hccp x authentication [no] hccp x revertive [no] hccp x reverttime [no] hccp x timers [no] hccp x track                 (here x: groupnumber ) </pre> <p>Assume that PRE-A is the active PRE and PRE-B is the standby PRE. When a switchover from PRE-A to PRE-B happens, PRE-A will be reset and rebooted. After rebooting, during the configuration, PRE-B will send its running-config over to PRE-A. This running-config will become PRE-A's startup-config. PRE-A will try to parse this configuration and start applying it. If the running-configuration on PRE-A was not saved before switchover, the user configured values of these commands will be absent.</p> <p>Workaround: Save the running-config to startup-config whenever the above commands are issued. This restriction will be relaxed in the next release.</p>

Table 83 Open Caveats for Cisco IOS Release 12.3(13a)BC4 (continued)

DDTS ID Number	Description
CSCsb14936	<p>SNMPv3 gets/sets fail following Performance Routing Engine (PRE) switchover. Attempts increment usmStatsWrongDigests.0.</p> <p>This issue exists in a configuration with RPR+ and that uses SNMPv3, where the snmp EngineID value is the default value.</p> <p>Workaround: Specify a value for the snmp EngineID via the global configuration CLI: <b>snmp-server engineID local</b> [octet string] where octet string is the desired engineID value.</p>
CSCsb17060	<p>The default cable modulation profile does not appear within the <b>show running-config</b> command even though the <b>cable modulation-profile</b> command is apparently configured.</p> <p>Workaround One: Configure the <b>cable modulation-profile initial</b> command.</p> <p>Workaround Two: Configure the <b>cable modulation-profile</b> command with no values.</p>
CSCsb20032	<p>After <b>shut</b> of an interface and then removal of legacy HA commands from the <b>shut</b> interface, a Performance Routing Engine (PRE) failover was performed from PREA --&gt; PREB. It was observed that after a PRE switchover, the corresponding PROTECT interface is now in *ACTIVE* state.</p> <p>There are no known workarounds.</p>
CSCsb26657	<p>The toaster feed_back context rate appears to be excessive when presented with multicast traffic.</p> <p>With a multicast group consisting of two members is presented with a rate of 10 multicast pps the feedback rate is at 50 cps. If changes are made to the group membership the feedback rate does not appear to change consistently with the change made.</p> <p>There are no known workarounds.</p>
CSCsb29527	<p>A Cisco uBR10000 series CMTS may not provide the full Minimum reserved rate configured for a downstream service flow.</p> <p>The issue may occur when the downstream channel of the cable interface that the modem is connected to is experiencing congestion.</p> <p>There are no known workarounds.</p>
CSCsb30593	<p>Per-modem downstream packet classifiers greater than 10 do not count matching packets.</p> <p>This issue only occurs when there are more than 10 packet classifiers on a single modem, a very rare configuration.</p> <p>There are no known workarounds.</p>

**Table 83** Open Caveats for Cisco IOS Release 12.3(13a)BC4 (continued)

DDTS ID Number	Description
CSCsb37557	<p>The term SNR in <b>show cable modem phy</b> and <b>show controller</b> is easily confused with CNR by customers.</p> <p>This issue occurs when running command <b>show cable modem phy</b> and <b>show controller</b>.</p> <p>There are no known workarounds.</p>
CSCsb40202	<p>The current implementation of cable filter groups can allow a CM or customer premises equipment (CPE) device to bypass filters.</p> <p>There are two cases where this issue can be triggered:</p> <ol style="list-style-type: none"> <li>1. MSO configures the CMTS with default cable filter groups with the <b>cable submgmt default filter-group</b> command and points them to a group ID that does not exist. IOS will not give a warning, and the device is completely open.</li> <li>2. DOCSIS1.1 provisioned CMs have TLV 37 configured, but points to a group ID that does not exist. IOS gives no warning, and the device is completely open.</li> </ol> <p>In cases where a group ID does not exist, default behavior of IOS should probably be a “deny all” like traditional ACLs instead of the current “permit all”.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(13a)BC4

Table 84 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC4.

**Table 84** Resolved Caveats for Cisco IOS Release 12.3(13a)BC4

DDTS ID Number	Description
CSCCek31085	<p>The interfaces.ifTable.ifEntry.ifSpeed MIB variable reports an invalid value for a 6.4 MHz, 64-QAM A-TDMA channel on a Cisco uBR10000 series router running Cisco IOS Release 12.2(15) BC2f or 12.3(13a)BC2.</p> <p>There are no known workarounds.</p>
CSCsc33372	<p>The following error message may appear after a cable modem termination system (CMTS) reload:</p> <p>UBR10000-3-NOMEM: Failed to get event buffer from flap-list event chunk</p> <p>There are no known workarounds.</p>
CSCsc44370	<p>CST: (Global HA) LC switchovers corrupts CM state.</p> <p>There are no known workarounds.</p>

Table 84 Resolved Caveats for Cisco IOS Release 12.3(13a)BC4 (continued)

DDTS ID Number	Description
CSCsc96651	<p>A Cisco uBR10012 router running Cisco IOS Release 12.3(13a)BC using the Policy-Based Routing (PBR) with <b>set ip default next-hop</b> does not function correctly when there is a default route (0.0.0.0) in the IP routing table. Instead of selecting the PBR next-hop address, the router selects and switches packets to the default route next-hop.</p> <p>Workaround: Remove the Default route (none) from the Routing Table will correct the PBR next-hop selection.</p> <p>Alternative workaround: Use <b>set ip next-hop</b> to provide the correct next-hop behavior.</p>
CSCsd03006	<p>The Cisco uBR10000 series router may experience tracebacks, bus errors or system hangs during online insertion and removal (OIR) operations when OIR-compatibility is enabled.</p> <p>This issue occurs when the OIR-compatibility feature is activated on a cable modem termination system (CMTS) line card that has one or more interfaces serving as a bundle master. The issue occurs when replacing an MC5x20 card with a compatible, but not identical, MC5x20. It does not occur when a card is replaced by an identical card type or if the OIR-compatibility feature is not enabled.</p> <p>Workaround: Remove the CMTS interface from the bundle prior to performing the OIR.</p>
CSCsd06576	<p>If <b>boot config config_file_name</b> is shown or is configured in the running-config, startup-config on the standby nvram is deleted. Even issuing <b>write mem</b> does not recreate the file, so when the standby becomes active, all configuration get wiped out.</p> <p>There are no known workarounds.</p>
CSCsd12954	<p>This caveat enables cloned modem detection message to be part of SYSLOG messages.</p>
CSCsd15546	<p>A Cisco router that is configured as a Dynamic Host Configuration Protocol (DHCP) relay may not append option 82 (that is, the Relay Agent option), even when the router is configured to do so in the following way:</p> <pre>ip dhcp relay information option no ip dhcp relay information check ip dhcp relay information trust-all</pre> <p>This issue occurs when the DHCP message contains an invalid option according to RFC 2132; for example, option 12 with length 0.</p> <p>Workaround: Ensure that the DHCP messages that is sent to the Cisco router functions as a DHCP relay contains valid options. If you cannot ensure this, there is no workaround.</p>
CSCsd18928	<p>Current cable modem termination system (CMTS) code allocates and frees up large blocks of memory for various CMTS functions, which exacerbates memory fragmentation issues in large Multi-System Operator (MSO) deployments.</p> <p>There are no known workarounds.</p>
CSCsc55372	<p>A cable modem termination system (CMTS) unexpectedly reloads in dialer function after issuing <b>show</b> commands.</p> <p>There are no known workarounds.</p>

**Table 84**      **Resolved Caveats for Cisco IOS Release 12.3(13a)BC4 (continued)**

DDTS ID Number	Description
CSCsd56351	<p>A cable modem gets stuck in the init(t) state when connected to a Cisco cable modem termination system (CMTS) running Cisco IOS Release 12.3(13a)BC2.</p> <p>This issue occurs when the registered modem goes offline, and the subsequent pre-registration packet's type-of-service (ToS) field from that cable modem is overwritten using the rules of the old DOCSIS configuration file. As a result, the tftp-ack packets are dropped on the next hop router due to an unexpected TOS field in packets. For packets from an unregistered cable modem, the ToS field should not be overwritten by CMTS.</p> <p>If the <b>clear cable modem H.H.H delete</b> command is executed from cable modem termination system (CMTS), the ToS field is not overwritten by CMTS.</p> <p>Workaround: Delete the stuck cable modem from CMTS by executing the following command, which will brings the stuck cable modem back into an online state:</p> <pre>clear cable modem mac-address delete</pre>
CSCsd62061	<p>The <b>cable dynamic-flow vrf name</b> command is not seen in the running configuration after a reload, but it is still seen in the startup-config file.</p> <p>This issue occurs after a reload.</p> <p>Workaround: Configure <b>cable dynamic-flow vrf name</b> at the interface.</p>
CSCsd65496	<p>A Cisco uBR router running Cisco IOS Release 12.3(9a)BC7 with 5cable-MC520s-d cards and packets generates NoSuchInstance errors when snmpget starts with ifInNUcastPkts. The ifInNUcastPkts is not populated for this ifType (docsCableUpstream) in the sparse ifTable.</p> <p>Workaround: Use snmpwalk or exclude object in the sparse ifTable (for example, ifInNUcastPkts, ifOutNUcastPkts, or ifOutQLen in snmpget).</p>
CSCsd84940	<p>For Cisco IOS Releases 12.3(17a)BC, 12.3(13)BC1, 12.3(13)BC2, 12.3(9a)BC8, the significant increase in number of upstream FEC errors may be seen when using MC16C or MC28C cards and these releases.</p> <p>The xxact degradation seen (if any) will depend up on plant conditions, and CMs and MTAs being used.</p> <p>There are no known workarounds.</p>
CSCej77130	<p>If a cable interface configuration is changed while a Hot Standby Connection-to-Connection Protocol (HCCP) static sync is occurring, a Performance Routing Engine (PRE) reload may occur.</p> <p>Workaround: Wait until the HCCP static sync is complete before changing the configuration.</p>
CSCek26121	<p>The sysUptime SNMP OID counter is reset after a Performance Routing Engine (PRE) switchover occurs.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(13a)BC3

Table 85 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC3.

**Table 85** Open Caveats for Cisco IOS Release 12.3(13a)BC3

DDTS ID Number	Description
CSCeh89315	The counters for leasequery-filter do not get cleared when <b>clear counters</b> or <b>clear counters cablex/y</b> is issued after the leasequery-filter related CLI have been unconfigured.  There are no known workarounds.
CSCei22859	The secondary service does not pass traffic after a line card switchover.  This issue is likely related to payload header suppression (PHS) traffic and switchovers.  Workaround: Do not use PHS.
CSCei31356	Packets from unknown subnets (src 0.0.0.0) are being forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.  There are no known workarounds.
CSCei54145	After Qos enforcement and modem reset, the modem takes the recently created profile and not the qos profile that was in use before modem reset.  There are no known workarounds.
CSCei54281	With N+1 switch overs, the number of expected customer premises equipment (CPE) devices does not get reflected in the <b>show cable modem verbose</b> command.  This issue occurs on a Performance Routing Engine (PRE) High Availability (HA) configuration  There are no known workarounds.
CSCei54358	When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.  This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.  There are no known workarounds.
CSCin92949	When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.  This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.  Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.
CSCin95131	Protector interface's modem entries would not be there in the docsIfCmtsMacToCmTable after multiple RPR/N+1 switchovers.  There are no known workarounds.

Table 85 Open Caveats for Cisco IOS Release 12.3(13a)BC3 (continued)

DDTS ID Number	Description
CSCsb02318	<p>The following Hot Standby Connection-to-Connection Protocol (HCCP) configuration commands may not preserve their non-default configuration values after two Performance Routing Engine (PRE) switchovers unless the running-config is saved to startup-config before PRE switchover.</p> <pre data-bbox="657 457 1161 609"> [no] hccp x authentication [no] hccp x revertive [no] hccp x reverttime [no] hccp x timers [no] hccp x track       (here x: groupnumber ) </pre> <p>Assume that PRE-A is the active PRE and PRE-B is the standby PRE. When a switchover from PRE-A to PRE-B happens, PRE-A will be reset and rebooted. After rebooting, during the configuration, PRE-B will send its running-config over to PRE-A. This running-config will become PRE-A's startup-config. PRE-A will try to parse this configuration and start applying it. If the running-configuration on PRE-A was not saved before switchover, the user configured values of these commands will be absent.</p> <p>Workaround: Save the running-config to startup-config whenever the above commands are issued. This restriction will be relaxed in the next release.</p>
CSCsb08548	<p>On a Cisco uBR10000 series platform, if IP packet debugging is turned on to match with any kind of access-list; than following console messages will be also displayed along with the debugs (if any):</p> <pre data-bbox="613 1039 1502 1291"> May 27 10:08:05.259: IP: recv fragment from 127.0.0.61 offset 0 bytes May 27 10:08:05.259: IP: recv fragment from 127.0.0.61 offset 1480 bytes May 27 10:08:06.339: IP: recv fragment from 127.0.0.51 offset 0 bytes May 27 10:08:06.343: IP: recv fragment from 127.0.0.51 offset 1480 bytes May 27 10:08:08.135: IP: recv fragment from 127.0.0.70 offset 0 bytes May 27 10:08:08.135: IP: recv fragment from 127.0.0.70 offset 1480 bytes ..... </pre> <p>Those above messages and ip packets are internal to the Cisco uBR10000 series router and never go out of the router.</p> <p>Workaround: It is not recommended to turn on ip packet debugging on huge routers such as the Cisco uBR10000 series router. If the user turn it on, than above intercommunication messages will also displayed along with debugs. To stop those messages user has to turn off ip packet debugging.</p>
CSCsb14936	<p>SNMPv3 gets/sets fail following Performance Routing Engine (PRE) switchover. Attempts increment usmStatsWrongDigests.0.</p> <p>This issue exists in a configuration with RPR+ and that uses SNMPv3, where the snmp EngineID value is the default value.</p> <p>Workaround: Specify a value for the snmp EngineID via the global configuration CLI: <b>snmp-server engineID local</b> [octet string] where <i>octet string</i> is the desired engineID value.</p>

Table 85 Open Caveats for Cisco IOS Release 12.3(13a)BC3 (continued)

DDTS ID Number	Description
CSCsb17060	<p>The default cable modulation profile does not appear within the <b>show running-config</b> command even though the <b>cable modulation-profile</b> command is apparently configured.</p> <p>Workaround One: Configure the <b>cable modulation-profile initial</b> command.</p> <p>Workaround Two: Configure the <b>cable modulation-profile</b> command with no values.</p>
CSCsb20032	<p>After <b>shut</b> of an interface and then removal of legacy HA commands from the <b>shut</b> interface, a Performance Routing Engine (PRE) failover was performed from PREA --&gt; PREB. It was observed that after a PRE switchover, the corresponding PROTECT interface is now in *ACTIVE* state.</p> <p>There are no known workarounds.</p>
CSCsb21814	<p>When using the downstream load balancing, utilization method, the cable modem termination system (CMTS ) will load balance using the max utilization upstream (US) or downstream (DS). For example, when one interface has a max utilization on the downstream, and the other has a max utilization on the upstream, CMTS moves all US traffic to one interface.</p> <p>There are no known workarounds.</p>
CSCsb26657	<p>The toaster feed_back context rate is excessive when multicast traffic is present.</p> <p>There are no known workarounds.</p>
CSCsb29527	<p>A Cisco uBR10000 series CMTS may not provide the full Minimum reserved rate configured for a downstream service flow.</p> <p>The issue may occur when the downstream channel of the cable interface that the modem is connected to is experiencing congestion.</p> <p>There are no known workarounds.</p>
CSCsb30593	<p>Per-modem downstream packet classifiers greater than 10 do not count matching packets.</p> <p>This issue only occurs when there are more than 10 packet classifiers on a single modem, a very rare configuration.</p> <p>There are no known workarounds.</p>

**Table 85** Open Caveats for Cisco IOS Release 12.3(13a)BC3 (continued)

DDTS ID Number	Description
CSCsb37557	<p>The term SNR in <b>show cable modem phy</b> and <b>show controller</b> is easily confused with CNR by customers.</p> <p>This issue occurs when running command <b>show cable modem phy</b> and <b>show controller</b>.</p> <p>There are no known workarounds.</p>
CSCsb40202	<p>The current implementation of cable filter groups can allow a CM or customer premises equipment (CPE) device to bypass filters.</p> <p>There are two cases where this issue can be triggered:</p> <ol style="list-style-type: none"> <li>1. MSO configures the CMTS with default cable filter groups with the <b>cable submgmt default filter-group</b> command and points them to a group ID that does not exist. IOS will not give a warning, and the device is completely open.</li> <li>2. DOCSIS 1.1 provisioned CMs have TLV 37 configured, but points to a group ID that does not exist. IOS gives no warning, and the device is completely open.</li> </ol> <p>In cases where a group ID does not exist, default behavior of IOS should probably be a “deny all” like traditional ACLs instead of the current “permit all”.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(13a)BC3

Table 86 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC3.

**Table 86** Resolved Caveats for Cisco IOS Release 12.3(13a)BC3

DDTS ID Number	Description
CSCsb16491	<p>A Cisco uBR10000 series router unexpectedly reloads when performing a <b>clear cable modem mac delete</b> while running ubr10k2-k9p6-mz.123-9a.BC3.bin.</p> <p>There are no known workarounds.</p>
CSCsd17301	<p>With Dynamic Message Integrity Check (DMIC) configured on the cable modem termination system (CMTS), the CMTS enters a state where all subsequent cable modem (CM) registration attempts fail and the CM ends up the in init(io) state. Cable modems that are online continue to work, but any cable modems that are reset, either by means of power-cycling or by the delete/reset CLI, do not work.</p> <p>This issue occurs if the Multi-System Operator (MSO) mistakenly provisions a modem configuration file that does not exist on the Trivial File Transfer Protocol (TFTP) server, and any modem tries to get online with CMTS using the non-existent configuration file.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(13a)BC2

Table 87 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC2.

**Table 87** Open Caveats for Cisco IOS Release 12.3(13a)BC2

DDTS ID Number	Description
CSCeh89315	<p>The counters for leasequery-filter do not get cleared when <b>clear counters</b> or <b>clear counters cablex/y</b> is issued after the leasequery-filter related CLI have been unconfigured.</p> <p>There are no known workarounds.</p>
CSCei22859	<p>The secondary service does not pass traffic after a line card switchover.</p> <p>This issue is likely related to payload header suppression (PHS) traffic and switchovers.</p> <p>Workaround: Do not use PHS.</p>
CSCei28619	<p>When there is around 30KPPS unicast traffic sent from the Cisco uBR10000 series router's upstream to a offline host , and the offline host has no ARP entry in the Cisco uBR10000 series router, the Cisco uBR10000 series router's pxf cpu queue will have high dropping rate. All hosts under the Cisco uBR10000 series router can not finish initial DHCP session.</p> <p>This issue occurs when 30KPPS unicast traffic is sent from a Cisco uBR10000 series router's upstream to a offline host. Average packet size is 64 bytes.</p> <p>Workaround: Add ARP entry for the unknown host.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are being forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCei54145	<p>After Qos enforcement and modem reset, the modem takes the recently created profile and not the qos profile that was in use before modem reset.</p> <p>There are no known workarounds.</p>
CSCei54281	<p>With N+1 switchovers, the number of expected customer premises equipment (CPE) devices does not get reflected in the <b>show cable modem verbose</b> command.</p> <p>This issue occurs in a Performance Routing Engine High Availability (HA) configuration.</p> <p>There are no known workarounds.</p>
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>

**Table 87**      **Open Caveats for Cisco IOS Release 12.3(13a)BC2 (continued)**

DDTS ID Number	Description
CSCin92949	<p>When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.</p> <p>This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.</p> <p>Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.</p>
CSCin95131	<p>Protector interface's modem entries would not be there in the docsIfCmtsMacToCmTable after multiple RPR/N+1 switchovers.</p> <p>There are no known workarounds.</p>
CSCsb02318	<p>The following Hot Standby Connection-to-Connection Protocol (HCCP) configuration commands may not preserve their non-default configuration values after two Performance Routing Engine (PRE) switchovers unless the running-config is saved to startup-config before PRE switchover.</p> <pre data-bbox="657 871 987 1024"> [no] hccp x authentication [no] hccp x revertive [no] hccp x reverttime [no] hccp x timers [no] hccp x track                 (here x: groupnumber ) </pre> <p>Assume that PRE-A is the active PRE and PRE-B is the standby PRE. When a switchover from PRE-A to PRE-B happens, PRE-A will be reset and rebooted. After rebooting, during the configuration, PRE-B will send its running-config over to PRE-A. This running-config will become PRE-A's startup-config. PRE-A will try to parse this configuration and start applying it. If the running-configuration on PRE-A was not saved before switchover, the user configured values of these commands will be absent.</p> <p>Workaround: Save the running-config to startup-config whenever the above commands are issued. This restriction will be relaxed in the next release.</p>

**Table 87 Open Caveats for Cisco IOS Release 12.3(13a)BC2 (continued)**

DDTS ID Number	Description
CSCsb08548	<p>On a Cisco uBR10000 series platform, if IP packet debugging is turned on to match with any kind of access-list; than following console messages will be also displayed along with the debugs (if any):</p> <pre> May 27 10:08:05.259: IP: recv fragment from 127.0.0.61 offset 0 bytes May 27 10:08:05.259: IP: recv fragment from 127.0.0.61 offset 1480 bytes May 27 10:08:06.339: IP: recv fragment from 127.0.0.51 offset 0 bytes May 27 10:08:06.343: IP: recv fragment from 127.0.0.51 offset 1480 bytes May 27 10:08:08.135: IP: recv fragment from 127.0.0.70 offset 0 bytes May 27 10:08:08.135: IP: recv fragment from 127.0.0.70 offset 1480 bytes .... </pre> <p>Those above messages and ip packets are internal to the Cisco uBR10000 series router and never go out of the router.</p> <p>Workaround: It is not recommended to turn on ip packet debugging on huge routers, such as the Cisco uBR10000 series router. If the user turn it on, than above intercommunication messages will also displayed along with debugs. To stop those messages user has to turn off ip packet debugging.</p>
CSCsb14936	<p>SNMPv3 gets/sets fail following Performance Routing Engine (PRE) switchover. Attempts increment usmStatsWrongDigests.0.</p> <p>This issue exists in a configuration with RPR+ and that uses SNMPv3, where the snmp EngineID value is the default value.</p> <p>Workaround: Specify a value for the snmp EngineID via the global configuration CLI: <b>snmp-server engineID local</b> [<i>octet string</i>] where <i>octet string</i> is the desired engineID value.</p>
CSCsb16491	<p>A Cisco uBR10000 series router unexpectedly reloads when performing a <b>clear cable modem mac delete</b> while running ubr10k2-k9p6-mz.123-9a.BC3.bin.</p> <p>There are no known workarounds.</p>
CSCsb17060	<p>The default cable modulation profile does not appear within the <b>show running-config</b> command even though the <b>cable modulation-profile</b> command is apparently configured.</p> <p>Workaround One: Configure the <b>cable modulation-profile initial</b> command.</p> <p>Workaround Two: Configure the <b>cable modulation-profile</b> command with no values.</p>
CSCsb20032	<p>After <b>shut</b> of an interface and then removal of legacy HA commands from the <b>shut</b> interface, a Performance Routing Engine (PRE) failover was performed from PREA --&gt; PREB. It was observed that after a PRE switchover, the corresponding PROTECT interface is now in *ACTIVE* state.</p> <p>There are no known workarounds.</p>

**Table 87**      **Open Caveats for Cisco IOS Release 12.3(13a)BC2 (continued)**

DDTS ID Number	Description
CSCsb21814	<p>When using the downstream load balancing, utilization method, the cable modem termination system (CMTS ) will load balance using the max utilization upstream (US) or downstream (DS). For example, when one interface has a max utilization on the downstream, and the other has a max utilization on the upstream, CMTS moves all US traffic to one interface.</p> <p>There are no known workarounds.</p>
CSCsb26657	<p>The toaster feed_back context rate is excessive when multicast traffic is present.</p> <p>There are no known workarounds.</p>
CSCsb27941	<p>A PacketCable call with Three Way Calling configured is distorted /lost after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCsb29527	<p>A Cisco uBR10000 series CMTS may not provide the full Minimum reserved rate configured for a downstream service flow.</p> <p>The issue may occur when the downstream channel of the cable interface that the modem is connected to is experiencing congestion.</p> <p>There are no known workarounds.</p>
CSCsb30593	<p>Per-modem downstream packet classifiers greater then 10 do not count matching packets.</p> <p>This issue only occurs when there are more than 10 packet classifiers on a single modem, a very rare configuration.</p> <p>There are no known workarounds.</p>
CSCsb37557	<p>The term SNR in <b>show cable modem phy</b> and <b>show controller</b> is easily confused with CNR by customers.</p> <p>This issue occurs when running command <b>show cable modem phy</b> and <b>show controller</b>.</p> <p>There are no known workarounds.</p>
CSCsb40202	<p>The current implementation of cable filter groups can allow a CM or customer premises equipment (CPE) device to bypass filters.</p> <p>There are two cases where this issue can be triggered:</p> <ol style="list-style-type: none"> <li>1. MSO configures the CMTS with default cable filter groups with the <b>cable submgmt default filter-group</b> command and points them to a group ID that does not exist. IOS will not give a warning, and the device is completely open.</li> <li>2. DOCSIS1.1 provisioned CMs have TLV 37 configured, but points to a group ID that does not exist. IOS gives no warning, and the device is completely open.</li> </ol> <p>In cases where a group ID does not exist, default behavior of IOS should probably be a “deny all” like traditional ACLs instead of the current “permit all”.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(13a)BC2

Table 88 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC2.

**Table 88** Resolved Caveats for Cisco IOS Release 12.3(13a)BC2

DDTS ID Number	Description
CSCea14522	<p>The following error message may appear when configuring:</p> <pre>%GENERAL-3-EREVENT: HWCEF: Loadinfo fastadj lock with NULL fasttag_rew -Traceback= 600E4B14 600E3490 60405FE0 604064A8 60D5E748 60D5938C 60E32D14 60D59604 60E2F724 60E2F9F0 60DE8A84 60DE8B2C 60E224F4 60E22B50 60DF30B4</pre> <p>This issue occurs on a Cisco UBR10000 CMTS with PRE2 running Cisco IOS Release 12.3(9a)BC7.</p> <p>This message appeared just after inserting the <b>ip route W.X.Y.Z M.A.S.K CableP/Q/0.R S.T.U.V</b> command to be used as a route-leaking for Internet access from the VPN (W.X.Y.Z and S.T.U.V are IP addresses, M.A.S.K is the mask and P,Q,R refer to the cable interface numbering).</p> <p>There are no known workarounds.</p>
CSCef28979	<p>If the host IP address is changed after the CM is online, the host IP address is not synched to the standby Performance Routing Engine (PRE) or Protect LC.</p> <p>This would cause delays in traffic recovery after a PRE or LC switchover.</p> <p>There are no known workarounds.</p>
CSCeg25277	<p>The primary Performance Routing Engine (PRE) on a Cisco uBR10000 series platform unexpectedly reloads in docsis classifier code.</p> <p>If there is secondary PRE, the secondary will take over and all the cable line cards get connected to secondary PRE. No cable modems went offline and service is restored as soon as routing converged on wan interface.</p> <p>There are no known workarounds.</p>
CSCeh73049	<p>A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.</p> <p>Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.</p> <p>This vulnerability is present in all versions of Cisco IOS that support the <b>tclsh</b> command.</p> <p>Workaround: This advisory with appropriate workarounds is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20060125-aaatel">http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20060125-aaatel</a></p>

**Table 88**      **Resolved Caveats for Cisco IOS Release 12.3(13a)BC2 (continued)**

DDTS ID Number	Description
CSCei04362	<p>Excessive UCD messages are sent for several minutes when upstream is coming up, possibly at a rate of 4ms interval.</p> <p>This issue occurs in a N+1 configuration when standby becomes active.</p> <p>There are no known workarounds.</p>
CSCei43076	<p>Deleting a CMTS subinterface, or reading the ifTable after a CMTS line card has been reset, causes a spurious memory access if the line card had one or more subinterfaces registered in the ifTable at the time of the reset.</p> <pre data-bbox="613 590 1523 716"> Address  Count  Traceback F8      786   0x608C6DA4 0x608C74F0 0x608C48D4 0x608C1AE8         0x60B9929C 0x60B9CBC8 0x60B8D140 0x60BB3500 88       1    0x608CE100 0x605603C8 0x6056418C 0x6051CB78         0x60180980 0x6052E2B4 0x605AB15C 0x605AB140 </pre> <p>Workaround: Manually delete the subinterfaces prior to resetting the line card and put them back after the reset.</p>
CSCei66602	<p>The line card may report an unexpected reload with load balancing enabled.</p> <p>There are no known workarounds.</p>
CSCei77471	<p>After multiple Hot Standby Connection-to-Connection Protocol (HCCP) switchovers, the Protect LC unexpectedly reloads when it becomes active. This issue occurs because the underlying Station Maintenance allocated for the virtual upstreams are not deallocated when the Protect LC is in standby mode, causing instability when the Protect LC switches back to active.</p> <p>When this issue occurs, the LC unexpectedly reloads and modems on that LC go offline until the Working LC takes over and goes in service.</p> <p>Workaround: Remove and do not support virtual upstream channels per Working LC interfaces.</p>
CSCej45500	<p>A cable modem attempting to come online with incorrect BPI+ credentials displays the following message in the log:</p> <pre data-bbox="613 1289 1523 1367"> SLOT 8/1: Oct 12 01:30:02.039: %UBR10000-3-MANUFACTURE_CA_CM_CERTIFICATE_FORMAT_ERROR: &lt;133&gt;CMTS [DOCSIS]: Manufacture CA Certificate Format Error </pre> <p>Workaround: For large systems, there are no known workarounds. It is very unlikely that the offending modem can be located without the MAC address information and broad based modem debug messages are likely to overwhelm the system and might cause an unexpected reload or Performance Routing Engine (PRE) failover.</p> <p>For small systems, perform the following:</p> <ol data-bbox="613 1583 1523 1764" style="list-style-type: none"> <li>1. look for modems failing to come online, in reject states, or not in online(pt) online(pk) and attempt to remove that modem from the network, or issue a DOCSIS 1.0 config file.</li> <li>2. Then try to code upgrade that modem.</li> <li>3. Enable debug messages for BPI+.</li> </ol>

**Table 88 Resolved Caveats for Cisco IOS Release 12.3(13a)BC2 (continued)**

DDTS ID Number	Description
CSCej63139	<p>If there is no secondary RKS server specified in gate-set, traceback will occur where NULL ptr is accessed. This can cause random reload on the system due to invalid memory access.</p> <p>Workaround: Specify the secondary RKS server in CA config.</p>
CSCej65202	<p>The standby Performance Routing Engine (PRE) unexpectedly reloads when the active PRE attempts to config sync the Hot Standby Connection-to-Connection Protocol (HCCP) Protect Interdb to it. This issue is specific to configuring sub-interfaces.</p> <p>When this issue occurs, the standby PRE will recover and return to HOT Standby mode. This does not affecting service on the active PRE.</p> <p>There are no known workarounds.</p>
CSCej66025	<p>When DS BW is saturated and no more CIR queue can be allocated on toaster, a new PacketCable Multimedia (PCMM) gate will be left in the committed state and use up gate resource.</p> <p>There are no known workarounds.</p>
CSCej68481	<p>Traceback and random Performance Routing Engine (PRE) reloads occur during LC switchover with PacketCable call having CALEA wiretap turned on.</p> <p>Workaround: Turn off CALEA wiretap.</p>
CSCej71974	<p>On a Cisco uBR10000 series router, the cable line card IPC may suddenly pause or hang for seconds, but the under layer IOS IPC still works. When this pause or hang is long enough, particular when the Performance Routing Engine (PRE) or BPE is busy, PRE will detect Cable line card timeout.</p> <p>This only occurs on the cable line card. Other line cards in the Cisco uBR10000 series router seem to work correctly.</p> <p>There are no known workarounds.</p>
CSCek03346	<p>Late Voice packets are observed to be further delayed, causing voice quality degradation.</p> <p>There are no known workarounds.</p>
CSCek06198	<p>Voice flows are shaped to their maximum configured bandwidth. This may shape voice packets arriving in a burst and cause voice quality degradation.</p> <p>There are no known workarounds.</p>
CSCsb25918	<p>On the MC520s card, signal-to-noise ratio (SNR) values may drop on a upstream causing modems to drop offline. They are running 16 QAM on the upstream.</p> <p>This issue occurs on a Cisco uBR10000series router running Cisco IOS Release 12.3(9a)BC1 with multiple MC520s cards. Switching modulation from 16-QAM to QPSK and back restored the SNR levels</p> <p>The Init Mtn Slots were increasing. Utilization on the upstreams did not differ.</p> <p>Workaround: Disable eq-coefficient, change modulation to qpsk, revert back to 16qam and re-enable eq-coefficient.</p>

**Table 88** *Resolved Caveats for Cisco IOS Release 12.3(13a)BC2 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb74615	Standby PRE2 stops responding when performing a reload on the active. This issue occurs when pre-configured SSM and tunnels are saved. There are no known workarounds.
CSCsb86672	Cable modems are online but the MTA is not getting IPs. Workaround: Microcode reload pxf.
CSCsc00363	Traceback occur repeatedly on PRE2. Sep 26 13:47:20.547: %GENERAL-3-EREVENT: No current_if_info for hwidb Cable7/0/0 icb 114688: subint 0 dlci_or_handle 1 <---Traceback---> Sep 26 13:47:25.947: %GENERAL-3-EREVENT: No current_if_info for hwidb Cable6/1/1 icb 106752: subint 0 dlci_or_handle 1 <---Traceback---> This issue occurs in Cisco IOS Release 12.3(9a)BC7 with PRE2 using multicast function. There are no known workarounds.
CSCsc02003	Unable to ping from Cisco uBR10000 (PRE2) to anything (DHCP server, modem, PC, etc.), and the Cisco uBR10000 router cannot forward any IP packet (except Fastethernet). PXF also appears to be stuck: Output of "show pxf dma" indicates the following errors. From RP Counters: Packets: 148, Cumulative Bytes: 12358 Output Drops: 0, Own Errors 22961, FromRP Interrupts 279309 PXF DMA New Work TTQ Full Error: 3258 PXF DMA FBTTQ Full Error: 3314 Output of "show pxf cpu context" indicates high cpu utilization. FP context utilization 1min            5min            60min ----- Actual                            99 %            99 %            94 % Theoretical                       98 %            98 %            55 % Maximum                           98 %            98 %            58 % This issue occurs under the following conditions: <ul style="list-style-type: none"> <li>• On Cisco IOS Release 12.3(9a)BC7 or 12.3(13a)BC with PRE2</li> <li>• On a PBR setting on cable interface</li> <li>• On a service-policy (LLQ) setting on Gigabit Ethernet interface</li> <li>• When pinging from PC to PC under CM during several minutes</li> </ul> Workaround: Reload the Cisco uBR10000 series router. However, this is a temporary workaround as the issue reproduces after reloading too.

**Table 88 Resolved Caveats for Cisco IOS Release 12.3(13a)BC2 (continued)**

DDTS ID Number	Description
CSCsc02416	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC6 may the following experience a bus error:</p> <p>System returned to ROM by bus error at PC 0x602BF6E4, address 0x4824 This issue occurs on a Cisco uBR10000 router running a PRE1 with MC28c &amp; MC520u cards and 15,000 attached devices.</p> <p>Workaround: Do not use the <b>cable modem mac addr access-group access group number</b> command on the Cisco uBR10000 series router. This command is not supported on the Cisco uBR10000 series router.</p>
CSCsc06630	<p>Executing the <b>hw-module subslot slot /subslot reset</b> command generates non-blocking request and destination port tracebacks:</p> <pre>*Oct 4 12:17:56.784: %REQGRP-3-SYSCALL: System call for command 6 (slot8/0) : Nonblocking request failed (Cause: timeout) -Traceback= 60378C84 606BFC84 606C226C 606C290C 606C3100 *Oct 4 12:18:02.368: %IPC-5-INVALID: Invalid dest port=0x0 -Traceback= 606C0508 606CC39C 606CC22C 606CC4A0 6067BBCC 6067C0D8 6067C59C</pre> <p>This issue occurs when the user resets a line card using either the <b>hw-module subslot reset</b> or <b>hw-module slot reset</b> command.</p> <p>There are no known workarounds.</p>
CSCsc07695	<p>Unable to ping PC-to-PC under cable modem with TLS setting.</p> <p>This issue is seen on Cisco IOS Release 12.3(9a)BC7 with TLS setting and occurs if the TLS setting is read from startup-config. However, there is no problem when setting it after booting.</p> <p>Workaround: Reset the <b>cable dot1q-vc-map</b> command.</p>
CSCsc11996	<p>A problem in the CMTS codebase may cause Cisco uBR10000 series routers to unexpectedly reload due to a memory corruption.</p> <p>This unexpected reload occurs in configurations using both IGMP and BPI+ when the number of multicast addresses assigned to a single multicast SID exceeds 119. The code supports a maximum of 8 multicast addresses per multicast SID per modem.</p> <p>Workaround: Use ip access lists to organize the multicast addresses into groups of eight. Then use the <b>cable match address</b> interface configuration command to create a multicast SAID for each group of addresses.</p>
CSCsc20781	<p>There will be a missing MIB entry (docsQoSServiceFlowPrimary) with VIB config.</p> <p>Workaround: Do not configured VIB.</p>

**Table 88** *Resolved Caveats for Cisco IOS Release 12.3(13a)BC2 (continued)*

DDTS ID Number	Description
CSCsc33766	<p>Modems fail to come online and reach init(d) state.</p> <p>An OIR of MC520 (S/U/T) where there is a change in card type (S/U/T), and the interfaces on the line card are Virtual Bundle members, will result in modems failing DHCP.</p> <p>Workaround: A shut/no shut of the affected Cable interfaces will allow the modems to come online.</p> <p>Alternative workaround: Remove the affected interfaces from the Bundle and add back to the bundle.</p>
CSCsc37564	<p>Cable intercept might not send copy of Downstream packets to the collection server. Only Upstream packets appear on the collection server.</p> <p>There are no known workarounds.</p>
CSCsc42019	<p>When configuring N+1 global with Virtual Interface Bundling, the Hot Standby Connection-to-Connection Protocol (HCCP) never goes into the ready state due to the following error:</p> <p>Static Sync is running, wait for another 1 min, renew hccp suspend timer HCCP keeps restarting its counters.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(13a)BC1

Table 89 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC1.

**Table 89** *Open Caveats for Cisco IOS Release 12.3(13a)BC1*

DDTS ID Number	Description
CSCCef28979	<p>If the host IP address is changed after the CM is online, the host IP address is not synched to the standby Performance Routing Engine (PRE) or Protect LC.</p> <p>This would cause delays in traffic recovery after a PRE or LC switchover.</p> <p>There are no known workarounds.</p>
CSCCef30185	<p>The following “Unknown type” error messages may appearing at the CMTS console after the following actions do N+1 switchover (or) shut/noshut on cable interface:</p> <p>Jul 29 09:06:44.899: Unknown type 16843263 Jul 29 09:06:44.899: Unknown type -16709634</p> <p>There are no known workarounds.</p>
CSCCef56516	<p>Signal-to-noise ratio (SNR) values can lower then expected with MC520u card.</p> <p>This issue occurs if virtual connectors 16,17,18,19 are used.</p> <p>There are no known workarounds.</p>

Table 89 Open Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)

DDTS ID Number	Description
CSCeg12791	<p>The CLI command <b>service-policy</b> causes the cable interface to become unresponsive. In some cases, a “Low on memory try again” message displays and eventually the device hangs. In other cases, the command can be issued successfully, but eventually the device stops responding.</p> <p>Workaround: Reboot the device.</p>
CSCeh89315	<p>The counters for leasequery-filter do not get cleared when <b>clear counters</b> or <b>clear counters cablex/y</b> is issued after the leasequery-filter related CLI have been unconfigured.</p> <p>There are no known workarounds.</p>
CSCei22859	<p>The secondary service does not pass traffic after a line card switchover.</p> <p>This issue is likely related to payload header suppression (PHS) traffic and switchovers.</p> <p>Workaround: Do not use PHS.</p>
CSCei28619	<p>When there is around 30KPPS unicast traffic sent from a Cisco uBR10000 series router's upstream to a offline host, and the offline host has no ARP entry in Cisco uBR10000 series router., the Cisco uBR10000 series router's pxf cpu queue will have high dropping rate. All host under the Cisco uBR10000 series router can not finish initial DHCP session.</p> <p>This issue occurs when 30KPPS unicast traffic is sent from the Cisco uBR10000 series router's upstream to a offline host. Average packet size is 64 bytes.</p> <p>Workaround: Add ARP entry for the unknown host.</p>
CSCei31356	<p>Packets from unknown subnets (src 0.0.0.0) are being forwarded by the cable modem termination system (CMTS), even if Unicast Reverse Path Forwarding (uRPF) is enabled.</p> <p>There are no known workarounds.</p>
CSCei54145	<p>After Qos enforcement and modem reset, the modem takes the recently created profile and not the qos profile that was in use before modem reset.</p> <p>There are no known workarounds.</p>
CSCei54281	<p>With N+1 switchovers, the number of expected customer premises equipment (CPE) devices does not get reflected in the <b>show cable modem verbose</b> command.</p> <p>This issue occurs in a Performance Routing Engine High Availability (HA) configuration.</p> <p>There are no known workarounds.</p>
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>

**Table 89**      **Open Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)**

DDTS ID Number	Description
CSCin92949	<p>When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.</p> <p>This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.</p> <p>Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.</p>
CSCin95131	<p>Protector interface's modem entries would not be there in the docsIfCmtsMacToCmTable after multiple RPR/N+1 switchovers.</p> <p>There are no known workarounds.</p>
CSCsa48673	<p>The Sh cable modem load-bal stat is 4294967295.</p> <p>There are no known workarounds.</p>
CSCsa50929	<p>The Fix for CSCsa48673 will cause US Load Balancing to not decrement the Pending count.</p> <p>There are no known workarounds.</p>
CSCsb02318	<p>The following Hot Standby Connection-to-Connection Protocol (HCCP) configuration commands may not preserve their non-default configuration values after two Performance Routing Engine (PRE) switchovers unless the running-config is saved to startup-config before PRE switchover.</p> <pre data-bbox="654 1079 987 1209"> [no] hccp x authentication [no] hccp x revertive [no] hccp x reverttime [no] hccp x timers [no] hccp x track </pre> <p style="text-align: center;">(here x: groupnumber )</p> <p>Assume that PRE-A is the active PRE and PRE-B is the standby PRE. When a switchover from PRE-A to PRE-B happens, PRE-A will be reset and rebooted. After rebooting, during the configuration, PRE-B will send its running-config over to PRE-A. This running-config will become PRE-A's startup-config. PRE-A will try to parse this configuration and start applying it. If the running-configuration on PRE-A was not saved before switchover, the user configured values of these commands will be absent.</p> <p>Workaround: Save the running-config to startup-config whenever the above commands are issued. This restriction will be relaxed in the next release.</p>

Table 89 Open Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)

DDTS ID Number	Description
CSCsb03768	<p>After locking ACTIVE (W) LC 5/0 and then performing a LC failover via <b>hw-module subslot 5/0 reset</b> card, 5/0 will now be in the STANDBY state once the card comes back online. All modem will failover to (P) 5/1.</p> <p>The following message was observed after trying to failover (P) 5/1 back to (W) 5/0:</p> <pre>Router#<b>redundancy linecard-group revertback 5/0</b> % HCCP 1 50: aborts switchover. Request later. % HCCP 2 50: aborts switchover. Request later. % HCCP 3 50: aborts switchover. Request later. % HCCP 4 50: aborts switchover. Request later. % HCCP 5 50: aborts switchover. Request later.</pre> <p><b>Workaround:</b> Perform a <b>hw-module subslot 5/1 reset</b> of the standby Protect card to failover the (P) 5/1 card back to (W) 5/0.</p>
CSCsb08548	<p>On a Cisco uBR10000 platform, if IP packet debugging is turned on to match with any kind of access-list; than following console messages will be also displayed along with the debugs(if any):</p> <pre>May 27 10:08:05.259: IP: recv fragment from 127.0.0.61 offset 0 bytes May 27 10:08:05.259: IP: recv fragment from 127.0.0.61 offset 1480 bytes May 27 10:08:06.339: IP: recv fragment from 127.0.0.51 offset 0 bytes May 27 10:08:06.343: IP: recv fragment from 127.0.0.51 offset 1480 bytes May 27 10:08:08.135: IP: recv fragment from 127.0.0.70 offset 0 bytes May 27 10:08:08.135: IP: recv fragment from 127.0.0.70 offset 1480 bytes ....</pre> <p>Those above messages and ip packets are internal to the Cisco uBR10000 series router and never go out of the router.</p> <p><b>Workaround:</b> It is not recommended to turn on ip packet debugging on huge routers, such as the Cisco uBR10000 series router. If the user turn it on, than above intercommunication messages will also displayed along with debugs. To stop those messages user has to turn off ip packet debugging.</p>
CSCsb14936	<p>SNMPv3 gets/sets fail following Performance Routing Engine (PRE) switchover. Attempts increment usmStatsWrongDigests.0.</p> <p>This issue exists in a configuration with RPR+ and that uses SNMPv3, where the snmp EngineID value is the default value.</p> <p><b>Workaround:</b> Specify a value for the snmp EngineID via the global configuration CLI: <b>snmp-server engineID local</b> [<i>octet string</i>] where <i>octet string</i> is the desired engineID value.</p>
CSCsb16491	<p>A Cisco uBR10000 series router unexpectedly reloads when performing a <b>clear cable modem mac</b> delete while running ubr10k2-k9p6-mz.123-9a.BC3.bin.</p> <p>There are no known workarounds.</p>

**Table 89**      **Open Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb17060	<p>The default cable modulation profile does not appear within the <b>show running-config</b> command even though the <b>cable modulation-profile</b> command is apparently configured.</p> <p>Workaround One: Configure the <b>cable modulation-profile initial</b> command.</p> <p>Workaround Two: Configure the <b>cable modulation-profile</b> command with no values.</p>
CSCsb20032	<p>After <b>shut</b> of an interface and then removal of legacy HA commands from the <b>shut</b> interface, a Performance Routing Engine (PRE) failover was performed from PREA --&gt; PREB. It was observed that after a PRE switchover, the corresponding PROTECT interface is now in *ACTIVE* state.</p> <p>There are no known workarounds.</p>
CSCsb20065	<p>Traceback was observed while booting up the secondary Performance Routing Engine (PRE).</p> <p>There are no known workarounds.</p>
CSCsb21814	<p>When using the downstream load balancing, utilization method, the cable modem termination system (CMTS ) will load balance using the max utilization upstream (US) or downstream (DS). For example, when one interface has a max utilization on the downstream, and the other has a max utilization on the upstream, CMTS moves all US traffic to one interface.</p> <p>There are no known workarounds.</p>
CSCsb25918	<p>On the MC520s card, signal-to-noise ratio (SNR) values may drop on a upstream causing modems to drop offline. They are running 16 QAM on the upstream.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC1 with multiple MC520s cards. Switching modulation from 16-QAM to QPSK and back restored the SNR levels</p> <p>The Init Mtn Slots were increasing. Utilization on the upstreams did not differ.</p> <p>Workaround: Disable eq-coefficient, change modulation to qpsk, revert back to 16qam and re-enable eq-coefficient.</p>
CSCsb26657	<p>The toaster feed_back context rate is excessive when multicast traffic is present.</p> <p>There are no known workarounds.</p>
CSCsb27941	<p>A PacketCable call with Three Way Calling configured is distorted /lost after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCsb29527	<p>A Cisco uBR10000 series CMTS may not provide the full Minimum reserved rate configured for a downstream service flow.</p> <p>The issue may occur when the downstream channel of the cable interface that the modem is connected to is experiencing congestion.</p> <p>There are no known workarounds.</p>

**Table 89**      **Open Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)**

DDTS ID Number	Description
CSCsb30593	<p>Per-modem downstream packet classifiers greater than 10 do not count matching packets.</p> <p>This issue only occurs when there are more than 10 packet classifiers on a single modem, a very rare configuration.</p> <p>There are no known workarounds.</p>
CSCsb35851	<p>On a Cisco uBR10000 CMTS, when a cable line card failover occurs, dynamic service flows associated with a dynamic service flow MPLS VPN lose their association to that VPN and revert back to being mapped to the “native” MPLS VPN of the cable modem.</p> <p>In addition, after a revertive failover from a Protect line card to a Working line card, new dynamic service flows are no longer linked to the correct MPLS VPN. Instead they are associated with the “native” MPLS VPN of the cable modem.</p> <p>There are no known workarounds.</p>
CSCsb37557	<p>The term SNR in <b>show cable modem phy</b> and <b>show controller</b> is easily confused with CNR by customers.</p> <p>This issue occurs when running command <b>show cable modem phy</b> and <b>show controller</b>.</p> <p>There are no known workarounds.</p>
CSCsb40202	<p>The current implementation of cable filter groups can allow a CM or customer premises equipment (CPE) device to bypass filters.</p> <p>There are two cases where this issue can be triggered:</p> <ol style="list-style-type: none"> <li>1. MSO configures the CMTS with default cable filter groups with the <b>cable submgmt default filter-group</b> command and points them to a group ID that does not exist. IOS will not give a warning, and the device is completely open.</li> <li>2. DOCSIS1.1 provisioned CMs have TLV 37 configured, but points to a group ID that does not exist. IOS gives no warning, and the device is completely open.</li> </ol> <p>In cases where a group ID does not exist, default behavior of IOS should probably be a “deny all” like traditional ACLs instead of the current “permit all”.</p> <p>There are no known workarounds.</p>
CSCsc44856	<p>After a Hot Standby Connection-to-Connection Protocol (HCCP) switchover, CEF may have adjfibs in the wrong VRF and incomplete adjacencies.</p> <p>This issue occurs on a Cisco uBR10000 series router with cable modem interface redundancy switching over from a subinterface in one VRF to an interface in a different VRF.</p> <p>There are no known workarounds.</p>

**Table 89** Open Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)

DDTS ID Number	Description
CSCsc48502	<p>The OIR-compatibility feature fails to restore shared upstream connector settings when exchanging compatible cable line cards (i.e. 520U to 520S).</p> <p>This issue occurs on an OIR of MC520 (S/U/T) where there is a change in card type (S/U/T), and one or more interfaces on the line card are configured to share upstream connectors.</p> <p>Workaround: Manually restore the configuration.</p>
CSCsc55518	<p>PRE2 unexpectedly reloads with the following error in the reload info:</p> <pre> PXF DMA Error - End of Descriptor Before Cmd Byte Length Exhausted There are no known workarounds. </pre>
CSCsc58373	<p>CISCO CMTS is needed to send random MPEG NULL frames. Certain chipset cable modems might not get a lock at DS 256QAM signal.</p> <p>There are no known workarounds.</p>
CSCsc62224	<p>A CMTS Running 12.3(13a)BC code will report a value of “unknown (4)” in the ifOperStatus and ifAdminStatus of Cable subinterfaces when queried by SNMP.</p> <p>This issue occurs when querying the ifTable of any CMTS which is configured with Cable subinterfaces. This affects any CMTS running 12.3(13a)BC code.</p> <p>There are no known workarounds.</p>
CSCsc64649	<p>Under heavy congestion, downstream packets may be dropped on 520 cable line cards. The packets may be dropped without regard to priority.</p> <p>There are no known workarounds.</p>
CSCsc68382	<p>The following error message may appear in the log of a Cisco uBR10000 series router:</p> <pre> %GENERAL-3-EREVENT: No current_if_info for hwidb Cable6/0/2 icb 98816: subint 1 dlci_or_handle 512 -Traceback= 600F6504 600DF07C 600E5F3C 600E6040 600E72A4 600E748C 60D5ECDC 60D5DF34 60D5F708 60406548 60D62A78 60408864 60408BE0 605718D0 605718B4 </pre> <p>This error occurs under the following conditions:</p> <ul style="list-style-type: none"> <li>• MPLS/VPN route leaking is configured</li> <li>• A cable interface belongs to a vrf with route-leaking</li> <li>• When customer premises equipment (CPE) behind a cable modem that is hanging of the above-mentioned cable interface gets an IP address through DHCP, the traceback is shown.</li> </ul> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(13a)BC1

Table 90 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC1.

**Table 90 Resolved Caveats for Cisco IOS Release 12.3(13a)BC1**

<b>DDTS ID Number</b>	<b>Description</b>
CSCeb46784	<p>PHS rules generated by DSA or DSC are not synched to the:</p> <ul style="list-style-type: none"> <li>• Protect LC</li> <li>• Standby Performance Routing Engine (PRE)</li> </ul> <p>There are no known workarounds.</p>
CSCeb62508	<p>Disk corruptions occurs to file system meta data (such as the FAT table, or directory entries).</p> <p>This issue may occur with Disk I/O errors, slow responses, or simultaneous accesses by multiple file systems.</p> <p>Workaround: Avoid multiple accesses to a disk.</p>
CSCeg74394	<p>The primary and backup FE or GE interfaces go into admin shutdown after a reload.</p> <p>While the router is coming backup after a reload, the console will display ethernets coming up and then going down, followed by a “shutdown” noticed under the configuration for both interfaces.</p> <p>This issue only occurs if a higher number FE or GE interface, such as FE0/3 or GE0/3, is configured as primary while a lower number interface, such as FE 0/2 or GE0/2, is configured as backup.</p> <p>This does not occur when the situation is reverse: when a lower number ethernet configured as primary and a higher number ethernet configured as backup.</p> <p>Also, one of the ethernet interfaces will loose its configured IP address and will be “no ip address” instead in the interface configuration.</p> <p>There are no known workarounds.</p>
CSCeh13489	<p>A router may reset its Border Gateway Protocol (BGP) session.</p> <p>This issue occurs when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.</p> <p>Workaround: Configure the <b>bgp maxas limit</b> command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.</p>
CSCeh64171	<p>After Performance Routing Engine (PRE) switchover, cable qos profile created by CM lost is found. Even after a <b>clear cable modem reset</b> is performed to let cable modem re-register.</p> <p>This issue occurs on PRE switchover.</p> <p>Workaround: <b>clear cable modem all reset</b> can get the qos profile back.</p>

**Table 90 Resolved Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)**

DDTS ID Number	Description
CSCei11912	<p>After a line card switchover, existing or new PacketCable calls do not work in an Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) environment.</p> <p>This issue occurs because the dynamic service flow ID (SFID) to VPN mapping is lost after a switchover. Hence, when dynamic service flows are created for new calls (after switchover), they get mapped to the VPN of either the cable modem or the Media Terminal Adapter (MTA) ,instead of the value that was configured in the configuration file or the CLI.</p> <p>There are no known workarounds.</p>
CSCei31900	<p>Modems using Baseline Privacy Interface Plus (BPI+) issue the following message and end up in the reject(pk) state.</p> <p>AUTH_REJECT_PERMANENT_AUTHORIZATION_FAILURE When the modem is individually reset using the <b>clear cable modem mac-address reset</b> command, it comes online(pt) without any other changes:</p> <pre data-bbox="613 823 1528 919">%UBR10000-3-AUTH_REJECT_PERMANENT_AUTHORIZATION_FAILURE: &lt;132&gt;CMTS [DOCSIS]:&lt;66030108&gt; Auth Reject - Permanent Authorization Failure . CM Mac Addr &lt;0004.bdaa.0000&gt;</pre> <p>This issue occurs when modem registration rates above 30 per second are sustained, more than 5000 modems are coming online at once, and high CPU usage (of over 50%) is occurring.</p> <p>In addition, trail drops may occur in the cable downstream default queues, and/or to the Route Processor (RP) queues.</p> <p>Workaround: After a cable modem termination system (CMTS) reload, or when this issue occurs, enter the following command:</p> <p><b>clear cable modem reject delete</b></p>
CSCei32426	<p>When Hot Standby Connection-to-Connection Protocol (HCCP) is configured, the Protect cable line card interface assumes the configuration of the Working cable line card interface upon a switchover. In that state, the Protect line card interface is active and has the configuration of the Working cable line card interface, including for example, the IP address.</p> <p>Should a <b>write memory</b> command be executed at this stage, such configuration would be saved, and cause a problem on the next reload. This is because we would have conflicting configurations (e.g. overlapping IP address between the Protect line card interface and the Working line card interface).</p> <p>This fix addresses the aforementioned issue, by not saving the non-hccp related configuration on the Protect line card interface, when a <b>write memory</b> command is issued while it is the active interface.</p> <p>There are no known workarounds.</p>
CSCei54307	<p>Traceback and alignment errors occur when executing show pxf cpu queue.</p> <p>There are no known workarounds.</p>

**Table 90 Resolved Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCei54858	<p>The skip af check flag should be set under the l2-vpn-service command.</p> <p>The potential problem from the current code is that when all l2-vpn configuration is removed from one ethernet interface, that skip flag will be cleared and causing other l2vpn service to other ethernet interface.</p> <p>There are no known workarounds.</p>
CSCei61732	<p>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.</p> <p>Cisco has made free software available that includes the additional integrity checks for affected customers.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-timers">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-timers</a></p>
CSCei73998	<p>DS secondary SF is not removed from the standby Performance Routing Engine (PRE) if the SF is deleted when it is in the reserved state. The SF is in the reserved state when it is created for a PC voice call and the call is put on hold.</p> <p>This issue occurs when a PC voice call is put on hold and then the call is terminated while on hold.</p> <p>There are no known workarounds.</p>
CSCei77416	<p>CMTS unexpectedly reloads when re-initialized a deleted bundle interface with existing configured subinterface.</p> <p>There are no known workarounds.</p>
CSCei81799	<p>The HCCP 7+1 global configuration feature (introduced in 12.3(13a)BC has swapped the definition of rfs1 &amp; rfs2. This is not consistent with the existing RF Switch configuration guide.</p> <p>If US10-US23 are shutdown and U0-U9 are switched over, all modems will go offline.</p> <p>Workaround: Change the IP addresses of rfs1 &amp; rfs2 using <b>ip host rfs# ip-address</b>.</p>
CSCei83154	<p>The OIR-compatibility feature is disabled if a secondary Performance Routing Engine (PRE) is installed.</p> <p>The presence of a secondary PRE in standby mode disables the OIR-compatibility setting.</p> <p>Workaround: Shutdown the secondary PRE before upgrading from an MC520S to an MC520u.</p>
CSCei86348	<p>RP may unexpectedly reload with the use of particular config file.</p> <p>There are no known workarounds.</p>

Table 90 Resolved Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)

DDTS ID Number	Description
CSCei87863	<p>With Multicast BPI+ enabled, multicast BPI+ streams may be refused by cable modems after the change of the access-list used for some BPI+ multicast groups because the MSAID/BPI_KEYS may be changed.</p> <p>This issue occurs if the configuration of an access-list, which is used in the <b>cable match ... bpi-enable</b> command, is change.</p> <p>Workaround: Reset the cable modem or the customer premises equipment (CPE) leaves the igmp group for several minutes. Or, instead of modifying existing ACL, add a new ACL with new cable match command.</p>
CSCej11541	<p>Bidirectional cable monitor ACL sniffing is not filtering data correctly. When data should have been blocked due to filtering, the data is being sent to the sniffer.</p> <p>This issue only occurs when bidirectional cable monitor ACL sniffing is enabled. Incoming and outgoing directions with same ACL filter OK.</p> <p>Workaround: If-console to the cable line card (CLC). The ACL has not reached the CLC. Please configured the ACL by hand on the CLC and then exit the if-console session. Now ACL data will filter properly.</p>
CSCej18695	<p>Some ACLs are not being deleted on the cable line card (CLC) after the NPE/Performance Routing Engine (PRE) issued a delete to the CLC. Also, extended ACL are received corrupted at the CLC.</p> <p>Workaround: Please if-console to the CLC and delete the ACL by hand using the ACL delete CLI on the CLC, or configure an extended ACL by hand on the CLC after deleting the garbage extended list on the CLC.</p> <p>If-console is a service internal command. You have to enable service internal on the CMTS first.</p> <p>Use <b>if-con slot/subslot</b> for line cards in a Cisco uBR10000 chassis.</p>
CSCej22163	<p>In a high availability configuration with multiple Performance Routing Engines (PREs), the standby PRE will occasionally reload when a card is removed from the active PRE's running configuration.</p> <p>The following command sequence is an example of the type of configuration changes that might cause the error to occur.</p> <pre>Router# <b>config t</b> Router(config)# <b>card 8/1 5cable-mc520s-d</b> Router(config)# <b>no card 8/1.</b> Router(config)#</pre> <p>There are no known workarounds.</p>
CSCej28478	<p>Committed gate is stuck and freed by CMTS in special CFNA call behavior by MTA. It can use up gate resource per subscriber and cause no further gate creation allowed per such subscriber.</p> <p>Workaround: Issue a <b>clear packetcable gate all</b> command. But this has an effect on clearing all gates on CMTS.</p>
CSCej30053	<p>When an extended ACL is configured for a specific host, cable monitor still filters all the traffic on the subnet of the specific host.</p> <p>This issue occurs under normal working conditions for cable monitor.</p> <p>There are no known workarounds.</p>

Table 90 Resolved Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)

DDTS ID Number	Description
CSCej35149	<p>When a named ACL used by cable monitor is deleted from RP card (NPE/Performance Routing Engine (PRE)), the cable line card (CLC) is supposed to delete the named ACL, but the CLC does not.</p> <p>This issue occurs under normal operation conditions.</p> <p>There are no known workarounds.</p>
CSCin97360	<p>Traffic through TLS tunnel fails after a Performance Routing Engine (PRE) switchover.</p> <p>Workaround: Disable and re-enable TLS config after Performance Routing Engine (PRE) switchover.</p>
CSCsa95245	<p>Configuration information is lost when an OIR operation involves different types of line cards. This is the expected behavior of IOS.</p> <p>Workaround: The normal procedure is to manually save the interface configuration prior to removing the line card and restore it after the OIR is complete.</p>
CSCsb02366	<p>QoS Prov for DOCSIS 2.0 cable modems very rightfully shows DOCSIS 1.0 or DOCSIS 1.1 because of the fact that the major difference between a modem running in DOCSIS 2.0 mode as opposed to DOCSIS 1.0/1.1 mode is the physical layer and not the QoS provisioning.</p> <p>In order to be consistent, we then should remove "DOC2.0" column under "QoS Provision" from <b>show cable modem mac summary</b> display.</p> <p>Additionally, we should also have <b>show cable modem phy summary</b> display to provide a quick summary of the cable modems in each phy mode on each interface.</p>
CSCsb05747	<p>FLAP-LIST is not aging properly in 12.3BC.</p> <p>There are no known workarounds.</p>
CSCsb21988	<p>When using file mode of SAMIS, the XML data appears corrupted.</p> <p>There are no known workarounds.</p>
CSCsb26840	<p>Packet drops on voice calls with PHS enabled when the maximum rate (MIR) for the voice stream is very close to the actual bandwidth used. You can notice this by picking up the phone and pressing a button. If you hear very short periods of silence interrupting the tone, that's it. Also, you can see if there are drops on the service flow by doing a <b>show interface cx/y/z service-flow n counters verbose</b> for the service flow corresponding to downstream voice data.</p> <p>This issue occurs when PHS is enabled.</p> <p>Workaround: Turn off PHS or use cable modems which have large maximum rates (MIR) for voice data.</p>
CSCsb28546	<p>Voice RTP/UDP packets are not forwarded to CALEA DF (Server) after Line Card or Performance Routing Engine (PRE) switchover is performed.</p> <p>There are no known workarounds.</p>

**Table 90 Resolved Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)**

DDTS ID Number	Description
CSCsb30694	<p>Repeated pxf unexpected reloads are observed with %PXF-2-FAULT: T1 Exception summary: CPU[t1r1c1]</p> <p>This issue occurs on a Cisco uBR10000 series router with a PRE1 platform running Cisco IOS Release 12.3(9a)BC3.</p> <p>There are no known workarounds.</p>
CSCsb37635	<p>CMTS unexpectedly reloads while the standby RP is loading.</p> <p>There are no known workarounds.</p>
CSCsb42361	<p>A Cisco uBR10000 series CMTS may suffer from high CPU in the IP Background process after adding a secondary IP address to a cable or bundle interface.</p> <p>The issue may occur when the number of ARP entries on the interface being configured is in the order of tens of thousands.</p> <p>The number of ARP entries on each interface may be approximately gauged with the following command:</p> <pre>show adjacency summary</pre> <p>Workaround: Ensure that secondary IP addresses are added during a maintenance window.</p> <p>Alternative workaround: Segment the CMTS into small cable interface bundle groups or to use separate subinterfaces so that a lower number of modems and Customer Premise Equipment ARP entries are linked to each subinterface.</p>
CSCsb42820	<p>5x20 line card is hanging in the “check_flap_list” function (%LCINFO-4-LCHUNG) causing a “power cycle” (%UBR10K-1-POWCYCLE).</p> <p>Workaround: Turn off all debugs, or excessive SNMP management of the system, to reduce the size of the flap list to 4000, and change the power-adjustment threshold to 4-6 dB.</p> <p>Alternative workaround: Enter “no logging console guaranteed” on RP and each line card.</p>
CSCsb53506	<p>Service flows that specify a max latency parameter may get less bandwidth than expected.</p> <p>If the max latency is specified (non-zero) and the minimum reserved rate is not perfectly divisible by 8000, the remainder of the division is not accounted for and the policer associated with the service flow's queue will rate limit packets at a rate below the minimum reserved rate.</p> <p>This can have a significant impact to voice flows as 10% of packets will be rate limited and voice quality will be lower than expected.</p> <p>PRE2 engine, not PRE1 max latency, must be non-zero minimum reserved rate must not be perfectly divisible by 8000.</p> <p>For example, if the standard bit rate of 87,200 bps for G.711 is used, it is vulnerable to the bug since it is not perfectly divisible by 8000.</p> <p>Workaround: Specify the minimum reserved rate to be a multiple of 8000.</p>

**Table 90 Resolved Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)**

DDTS ID Number	Description
CSCsb63551	<p>When examining the local CMTS uBR100012, the router log the following messages:</p> <pre data-bbox="574 394 857 415">%AMDP2_FE-6-EXCESSCOLL</pre> <p>This issue can occur under normal operating conditions and with light load. This fix will correct these errors.</p> <p>There are no known workarounds.</p>
CSCsb71967	<p>After the reboot, the config on the specific upstreams have changed from 3200000 to 1600000 in 2 specific upstreams.</p> <p>This issue is seen in cable-MC16c cards in 12.3(13a)BC when spectrum-group is configured (not seen in 12.3(9a)BC).</p> <p>Workaround: configure 3200000 manually in the affected upstreams manually after reboot.</p>
CSCsb74136	<p>An unexpected reload will occur when using old Flash Memory and old-style PCMCIA cards like slot0: and slot1: with a small value for the <b>cable sflog</b> command.</p> <p>It is advised that, while using SAMIS, to use newer ATA style PCMCIA cards. Also, the recommended value for the <b>sflog</b> command is as below to obtain deleted service flows. If other values are used, sflog file might need to be created in the filesystem and with slot0: and slot1: being used for the sflog file, the unexpected reload might occur:</p> <pre data-bbox="574 1050 1188 1071">cable sflog max-entry 40000 entry-duration 86400</pre> <p>Workarounds: Use <b>cable sflog max-entry 40000 entry-duration 86400</b> to collect the deleted service flow information in SAMIS.</p> <p>Alternative workaround: Use newer ATA style flash cards like disk0:, disk1:</p>
CSCsb76288	<p>The <b>card</b> configuration command is not always propagated to the standby Performance Routing Engine (PRE) if OIR-compatibility is enabled. This results in a configuration mismatch between the standby and active PREs where the card is present in the running configuration of the active PRE but not in the standby PRE.</p> <p>This issue occurs when the OIR-compatibility is enabled on the slot, and the <b>card</b> command is specified an MC520 type line card.</p> <p>Workaround: Re-issue the <b>no card slotsubslot</b> command followed by the <b>card slotsubslot cardtype</b> command.</p>
CSCsb76299	<p>A given service class when added to admission control configuration, may not take effect.</p> <p>This issue occurs if the name of the service class is exactly 15 characters long.</p> <p>Workaround: Make the service class name shorter than 15 characters.</p>
CSCsb76667	<p>GE link flap with TLS (Transparent LAN Service) after N+1 switchover, so end-to-end TLS traffic fail for a few seconds.</p> <p>This issue occurs on Cisco IOS Releases 12.3(9a)BC6 and 12.3(13a)BC and configured TLS and N+1 environment.</p> <p>There are no known workarounds.</p>

**Table 90** Resolved Caveats for Cisco IOS Release 12.3(13a)BC1 (continued)

DDTS ID Number	Description
CSCsb96390	<p>When running Cisco IOS Release 12.3(13a)BC on a Cisco uBR10012 CMTS configured for N+1 redundancy, MPLS, and PacketCable calls switchover scenarios can cause calls to drop and also modems to go offline when they should remain online.</p> <p>This issue occurs on an Cisco uBR10012 router running RF line card redundancy with MPLS and PacketCable configured. Initiate RF line card switchovers with OIR, test crash, or CLI.</p> <p>There are no known workarounds.</p>
CSCsb99726	<p>The Cisco router may not be able to utilize the full DS bandwidth on a 520 line card.</p> <p>This issue occurs when multiple BE service flows try to utilize the full DS bandwidth on a 520 line card.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(13a)BC

Table 91 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC.

**Table 91** Open Caveats for Cisco IOS Release 12.3(13a)BC

DDTS ID Number	Description
CSCef28979	<p>If the host IP address is changed after the CM is online, the host IP address is not synched to the standby Performance Routing Engine (PRE) or Protect LC.</p> <p>This would cause delays in traffic recovery after a PRE or LC switchover.</p> <p>There are no known workarounds.</p>
CSCef30185	<p>The following “Unknown type” error messages may appearing at the CMTS console after the following actions do N+1 switchover (or) shut/noshut on cable interface:</p> <pre>Jul 29 09:06:44.899: Unknown type 16843263 Jul 29 09:06:44.899: Unknown type -16709634</pre> <p>There are no known workarounds.</p>
CSCeg12791	<p>The CLI command <b>service-policy</b> causes the cable interface to become unresponsive. In some cases, a “Low on memory try again” message displays and eventually the device hangs. In other cases, the command can be issued successfully, but eventually the device stops responding.</p> <p>Workaround: Reboot the device.</p>
CSCeg59363	<p>QoS provisioning mode may not appear correct after a Performance Routing Engine (PRE) switchover. This is a display problem and the Cisco uBR10000 series router will continue to behave normally.</p> <p>There are no known workarounds.</p>

Table 91 Open Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCeh36260	<p>When configuring the Cisco uBR10000 series router by pasting all cable configurations, an Hot Standby Connection-to-Connection Protocol (HCCP) LC config flag is not synched to the standby Performance Routing Engine (PRE). This will cause LCs to go non-functional after a PRE switchover.</p> <p>Workaround One: Wait for the Cable line-cards to boot up, then start the pasting of configurations.</p> <p>Workaround Two: Complete the configuration on the active PRE and then issue <b>hw module sec-cpu reset</b> to reset the standby PRE.</p>
CSCeh59829	<p>Traceback appears in output of <b>show tech</b>:</p> <pre>%GENERAL-3-EREVENT: pxf_drop_interface: No c10k_tt_hwdb</pre> <p>This issue occurs when executing the CLI command <b>show tech</b>. This is a rare occurrence and has no negative impact on the system.</p> <p>There are no known workarounds.</p>
CSCeh64171	<p>After Performance Routing Engine (PRE) switchover, cable qos profile created by CM lost is found. Even after a <b>clear cable modem reset</b> is performed to let cable modem re-register.</p> <p>This issue occurs on PRE switchover.</p> <p>Workaround: <b>clear cable modem all reset</b> can get the qos profile back.</p>
CSCeh89315	<p>The counters for leasequery-filter do not get cleared when <b>clear counters</b> or <b>clear counters cablex/y</b> is issued after the leasequery-filter related CLI have been unconfigured.</p> <p>There are no known workarounds.</p>
CSCeh97801	<p>In multitiered US CIR, some cases the function and fairness do not work.</p> <p>There are no known workarounds.</p>
CSCei18492	<p>When a large number of modems are registering, the cable line-cards may timeout and reset.</p> <p>There are no known workarounds.</p>
CSCei22859	<p>The secondary service does not pass traffic after a line card switchover.</p> <p>This issue is likely related to payload header suppression (PHS) traffic and switchovers.</p> <p>Workaround: Do not use PHS.</p>
CSCei28619	<p>When there is around 30KPPS unicast traffic sent from the Cisco uBR10000 series router's upstream to a offline host, and the offline host has no ARP entry in the Cisco uBR10000 series router, the Cisco uBR10000 series router's pxf cpu queue will have high dropping rate. All host under the Cisco uBR10k series router can not finish initial DHCP session.</p> <p>This issue occurs when 30KPPS unicast traffic is sent from Cisco uBR10000 series router's upstream to a offline host. Average packet size is 64 bytes.</p> <p>Workaround: Add ARP entry for the unknown host.</p>



Table 91 Open Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCei39591	<p>After selecting 200 KHz upstream channel width on an upstream, all future upstream channel width changes on MC520 cards; causing all modems offline with T4 timeout.</p> <p>This issue occurs when manually configuring the upstream channel width on the MC520 card to something other than it was previously.</p> <p>Workaround: Do not use upstream channel width of 200 KHz.</p>
CSCei45247	<p>RP CPU on the Cisco uBR10000 series router is high with large modem / customer premises equipment (CPE) counts:</p> <pre>cable cmcpe-list valid-time &lt;time&gt;</pre> <p>is configured to a value less than the defaults</p> <p>This issue occurs when more than 10,000 modems, or more than 30,000 CPE devices are on a single MC520card.</p> <p>The cable cmcpe-list valid-time 10 line card may become unresponsive, and could fail due to missed keepalive messages under certain typical traffic conditions</p> <p>Workaround: Return the configuration to the default setting of 900 seconds (15 minutes).</p>
CSCei49230	<p>The line card may become unresponsive when reloading the Cisco uBR10012 chassis, and when the Cisco uBR10012 router is at ROMMON. When both TCC+ cards are not present (shutdown or unplugged), and one route processor (RP) card is active, the other one is in ROMMON mode. Rebooting the active RP card in this circumstance causes the line card to unexpectedly reload.</p> <p>To avoid this behavior, ensure that at least one TCC+ card is installed and operational on the Cisco uBR10012 router. Refer to the Cisco uBR10012 Universal Broadband Router TCC+ Card document on Cisco.com:</p> <p><a href="http://www.cisco.com/en/US/docs/interfaces_modules/cable/installation/tcc5094.html">http://www.cisco.com/en/US/docs/interfaces_modules/cable/installation/tcc5094.html</a></p>
CSCei54145	<p>After Qos enforcement and modem reset, the modem takes the recently created profile and not the qos profile that was in use before modem reset.</p> <p>There are no known workarounds.</p>
CSCei54196	<p>CM created Qos profile cannot be enforced.</p> <p>Qos profile enforcement does not work in the following cases:</p> <ol style="list-style-type: none"> <li>1. From mgmt profile to CM profile</li> <li>2. From one CM profile to another CM profile</li> </ol> <p>There are no known workarounds.</p>
CSCei54281	<p>With N+1 switchovers, the number of expected customer premises equipment (CPE) devices does not get reflected in the <b>show cable modem verbose</b> command.</p> <p>This issue occurs in a Performance Routing Engine High Availability (HA) configuration.</p> <p>There are no known workarounds.</p>
CSCei54307	<p>Traceback and alignment errors occur when executing show pxf cpu queue.</p> <p>There are no known workarounds.</p>

**Table 91**      **Open Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCei54358	<p>When a line card switchover is performed with 254 hosts, tracebacks occur and modems stop forwarding traffic.</p> <p>This issue occurs only when there are 254 hosts in a Performance Routing Engine High Availability (HA) N+1 configuration.</p> <p>There are no known workarounds.</p>
CSCin92057	<p>The ifInBroadcastPkts MIB counters will not increment if VIB config is turned on.</p> <p>There are no known workarounds.</p>
CSCin92949	<p>When using MC520u cards, customer premises equipment (CPE) traffic to the cable modem termination system (CMTS) interface fails.</p> <p>This issue is caused by a mismatch between the filter-groups specified in the cable-modem (CM)-registration files and the filter-groups configured on the CMTS. If a specified filter-group does not exist on the CMTS, the CMTS or the toaster could unexpectedly reload.</p> <p>Workaround: All filter-groups specified in the CM-registration files MUST exist on the CMTS.</p>
CSCin95131	<p>Protector interface's modem entries would not be there in the docsIfCmtsMacToCmTable after multiple RPR/N+1 switchovers.</p> <p>There are no known workarounds.</p>
CSCin95168	<p>Line card may unexpectedly reload after running Qos profile script.</p> <p>There are no known workarounds.</p>
CSCsa50929	<p>The Fix for CSCsa48673 will cause US Load Balancing to not decrement the Pending count.</p> <p>There are no known workarounds.</p>
CSCsa77241	<p>Outbound access list does not increment counters when denying multicast echo packets.</p> <p>There are no known workarounds.</p>

**Table 91 Open Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCsb02318	<p>The following Hot Standby Connection-to-Connection Protocol (HCCP) configuration commands may not preserve their non-default configuration values after two Performance Routing Engine (PRE) switchovers unless the running-config is saved to startup-config before PRE switchover.</p> <pre data-bbox="618 457 1122 611"> [no] hccp x authentication [no] hccp x revertive [no] hccp x reverttime [no] hccp x timers [no] hccp x track                     (here x: groupnumber )                     </pre> <p>Assume that PRE-A is the active PRE and PRE-B is the standby PRE. When a switchover from PRE-A to PRE-B happens, PRE-A will be reset and rebooted. After rebooting, during the configuration, PRE-B will send its running-config over to PRE-A. This running-config will become PRE-A's startup-config. PRE-A will try to parse this configuration and start applying it. If the running-configuration on PRE-A was not saved before switchover, the user configured values of these commands will be absent.</p> <p>Workaround: Save the running-config to startup-config whenever the above commands are issued. This restriction will be relaxed in the next release.</p>
CSCsb02508	<p>SNMP cannot poll for docsQosServiceFlowPrimary for non-master Cable bundled interface.</p> <p>There are no known workarounds.</p>
CSCsb03768	<p>After locking ACTIVE (W) LC 5/0 and then performing a LC failover via <b>hw-module subslot 5/0 reset</b> card, 5/0 will now be in the STANDBY state once the card comes back online. All modem will failover to (P) 5/1.</p> <p>The following message was observed after trying to failover (P) 5/1 back to (W) 5/0:</p> <pre data-bbox="574 1234 1175 1388"> Router#<b>redundancy linecard-group revertback 5/0</b> % HCCP 1 50: aborts switchover. Request later. % HCCP 2 50: aborts switchover. Request later. % HCCP 3 50: aborts switchover. Request later. % HCCP 4 50: aborts switchover. Request later. % HCCP 5 50: aborts switchover. Request later.                     </pre> <p>Workaround: Perform a <b>hw-module subslot 5/1 reset</b> of the standby Protect card to failover the (P) 5/1 card back to (W) 5/0.</p>
CSCsb05747	<p>The FLAP-LIST is not aging properly in Cisco IOS Release 12.3BC.</p> <p>There are no known workarounds.</p>
CSCsb06638	<p>With upstream utilization load balancing configured, modems are not being moved to balance the traffic.</p> <p>There are no known workarounds.</p>

Table 91 Open Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCsb08548	<p>On a Cisco uBR10000 series platform, if IP packet debugging is turned on to match with any kind of access-list; than following console messages will be also displayed along with the debugs (if any):</p> <pre>May 27 10:08:05.259: IP: recv fragment from 127.0.0.61 offset 0 bytes May 27 10:08:05.259: IP: recv fragment from 127.0.0.61 offset 1480 bytes May 27 10:08:06.339: IP: recv fragment from 127.0.0.51 offset 0 bytes May 27 10:08:06.343: IP: recv fragment from 127.0.0.51 offset 1480 bytes May 27 10:08:08.135: IP: recv fragment from 127.0.0.70 offset 0 bytes May 27 10:08:08.135: IP: recv fragment from 127.0.0.70 offset 1480 bytes .....</pre> <p>Those above messages and ip packets are internal to the Cisco uBR10000 series router and never go out of the router.</p> <p>Workaround: It is not recommended to turn on ip packet debugging on huge routers, such as the Cisco uBR10000 series router. If the user turn it on, than above intercommunication messages will also displayed along with debugs. To stop those messages user has to turn off ip packet debugging.</p>
CSCsb14936	<p>SNMPv3 gets/sets fail following Performance Routing Engine (PRE) switchover. Attempts increment usmStatsWrongDigests.0.</p> <p>This issue exists in a configuration with RPR+ and that uses SNMPv3, where the snmp EngineID value is the default value.</p> <p>Workaround: Specify a value for the snmp EngineID via the global configuration CLI: <b>snmp-server engineID local [octet string]</b> where <i>octet string</i> is the desired engineID value.</p>
CSCsb16491	<p>A Cisco uBR10000 series router unexpectedly reloads when performing a <b>clear cable modem mac</b> delete while running ubr10k2-k9p6-mz.123-9a.BC3.bin.</p> <p>There are no known workarounds.</p>
CSCsb17060	<p>The default cable modulation profile does not appear within the <b>show running-config</b> command even though the <b>cable modulation-profile</b> command is apparently configured.</p> <p>Workaround One: Configure the <b>cable modulation-profile initial</b> command.</p> <p>Workaround Two: Configure the <b>cable modulation-profile</b> command with no values.</p>
CSCsb20032	<p>After <b>shut</b> of an interface and then removal of legacy HA commands from the <b>shut</b> interface, a Performance Routing Engine (PRE) failover was performed from PREA --&gt; PREB. It was observed that after a PRE switchover, the corresponding PROTECT interface is now in *ACTIVE* state.</p> <p>There are no known workarounds.</p>
CSCsb20065	<p>Traceback was observed while booting up the secondary Performance Routing Engine (PRE).</p> <p>There are no known workarounds.</p>

**Table 91** Open Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCsb21814	<p>When using downstream load balancing, utilization method, CMTS will load balance using the max utilization, US or DS. When one interface has a max utilization on the DS, and the other has a max utilization on the upstream; CMTS will move all us traffic to one interface.</p> <p>There are no known workarounds.</p>
CSCsb25918	<p>On the MC520s card, signal-to-noise ratio (SNR) values may drop on a upstream causing modems to drop offline. They are running 16 QAM on the upstream.</p> <p>This issue occurs on an Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC1 with multiple MC520s cards. Switching modulation from 16-QAM to QPSK and back restored the SNR levels</p> <p>The Init Mtn Slots were increasing. Utilization on the upstreams did not differ.</p> <p>Workaround: Disable eq-coefficient, change modulation to qpsk, revert back to 16qam and re-enable eq-coefficient.</p>
CSCsb26657	<p>The toaster feed_back context rate is excessive when multicast traffic is present.</p> <p>There are no known workarounds.</p>
CSCsb27930	<p>A PacketCable call with Calling Waiting configured is lost after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCsb27941	<p>A PacketCable call with Three Way Calling configured is distorted /lost after a line card switchover.</p> <p>There are no known workarounds.</p>
CSCsb28008	<p>A PacketCable call with Calling Waiting configured is distorted/lost after a Performance Routing Engine (PRE) switchover.</p> <p>There are no known workarounds.</p>
CSCsb28482	<p>When connector 19 is configured with default connectors (for Cable X/0/4, upstream 3), the signal-to-noise ratio (SNR) is around 29dB. When Connector 19 is configured for Cable X/0/0, upstream 3, SNR is around 16dB - 18dB.</p> <p>This issue is related to CSCef56516.</p> <p>There are no known workarounds.</p>
CSCsb29361	<p>In some circumstances, a cable modem with a downstream minimum reserved rate is allowed to register on a Cisco uBR10000 series cable modem termination system (CMTS). However, committed information rate (CIR) resources for the modem are not available. Error messages similar to the following are displayed in the unit's log:</p> <pre>%UBR10K-3-QALLOCFAIL_INFO: Failure to allocate QoS queue: Request CIR exceeds available link rate. %UBR10K-3-QALLOCFAIL: Failure to allocate QoS queue for service flow 236, CM 0004.9e95.f2a9</pre> <p>The modem is not able to receive any downstream data.</p> <p>The issue occurs only when the total reserved downstream bandwidth approaches the total available downstream bandwidth.</p> <p>There are no known workarounds.</p>

**Table 91**      **Open Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCsb29527	<p>A Cisco uBR10000 series CMTS may not provide the full Minimum reserved rate configured for a downstream service flow.</p> <p>The issue may occur when the downstream channel of the cable interface that the modem is connected to is experiencing congestion.</p> <p>There are no known workarounds.</p>
CSCsb29718	<p>The customer premises equipment (CPE) does not complete the Dynamic Host Configuration Protocol (DHCP) when moved from behind one cable modem to another.</p> <p>The following event is logged:</p> <pre> ...start... Jun 30 13:48:54.962: %UBR10000-3-SPOOFEDMAC: Investigating MAC=0011.2f32.c220 Cable6/1/0 sid 2900: Original MAC on sid 2899 Cable6/1/0 ...end... </pre> <p>Workaround: Enter the <b>clear cable modem</b> or <b>clear cable host</b> command.</p>
CSCsb30593	<p>Per-modem downstream packet classifiers greater than 10 do not count matching packets.</p> <p>This issue only occurs when there are more than 10 packet classifiers on a single modem, a very rare configuration.</p> <p>There are no known workarounds.</p>
CSCsb30694	<p>Repeated pxf unexpected reloads occur with the %PXF-2-FAULT: T1 Exception summary: CPU[t1r1c1]</p> <p>This issue occurs on a Cisco uBR10000 series router with a PRE1 platform running Cisco IOS Release 12.3(9a)BC3.</p> <p>There are no known workarounds.</p>
CSCsb31039	<p>While verifying E911 call stability, the active Performance Routing Engine (PRE) crashed after LC switchover.</p> <p>There are no known workarounds.</p>
CSCsb35851	<p>On a Cisco uBR10000 CMTS, when a cable line card failover occurs, dynamic service flows associated with a dynamic service flow MPLS VPN lose their association to that VPN and revert back to being mapped to the “native” MPLS VPN of the cable modem.</p> <p>In addition, after a revertive failover from a Protect line card to a Working line card, new dynamic service flows are no longer linked to the correct MPLS VPN. Instead they are associated with the “native” MPLS VPN of the cable modem.</p> <p>There are no known workarounds.</p>
CSCsb37557	<p>The term SNR in <b>show cable modem phy</b> and <b>show controller</b> is easily confused with CNR by customers.</p> <p>This issue occurs when running command <b>show cable modem phy</b> and <b>show controller</b>.</p> <p>There are no known workarounds.</p>

**Table 91**      **Open Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCsb37635	<p>CMTS unexpectedly reloads while the standby RP is loading.</p> <p>There are no known workarounds.</p>
CSCsb38906	<p>In logs, the following messages appears:</p> <pre data-bbox="574 449 1162 499">%C10K_QUEUE_CFG_GENERAL-3-EREVENT: Error @ ./toaster/c10k_rp/c10kcr1_tt_queue_cfg.c:1276</pre> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC3.</p> <p>There are no known workarounds.</p>
CSCsb40009	<p>The line card may unexpectedly reload during boot up.</p> <p>There are no known workarounds.</p>
CSCsb40202	<p>The current implementation of cable filter groups can allow a CM or customer premises equipment (CPE) device to bypass filters.</p> <p>There are two cases where this issue can be triggered:</p> <ol data-bbox="574 835 1489 1035" style="list-style-type: none"> <li>1. MSO configures the CMTS with default cable filter groups with the <b>cable submgmt default filter-group</b> command and points them to a group ID that does not exist. IOS will not give a warning, and the device is completely open.</li> <li>2. DOCSIS1.1 provisioned CMs have TLV 37 configured, but points to a group ID that does not exist. IOS gives no warning, and the device is completely open.</li> </ol> <p>In cases where a group ID does not exist, default behavior of IOS should probably be a “deny all” like traditional ACLs instead of the current “permit all”.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(13a)BC

Table 92 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(13a)BC.

**Table 92**      *Resolved Caveats for Cisco IOS Release 12.3(13a)BC*

DDTS ID Number	Description
CSCec48810	<p>When a service policy is applied to the interface, traffic will be dropped in the default queue. A reload will fix this problem and the router is functioning as it should.</p> <p>If you then remove and add the service policy again to the interface, it works correctly. To reproduce the problem again you have to reload the box without the service policy applied to the interface and apply the service policy again after the reload.</p> <p>This issue occurs on a Cisco uBR 10000 series router running Cisco IOS Release 12.2(16)BX1.</p> <p>Workaround: Reload the router after applying the service-policy.</p>
CSCed53225	<p>Due to excessive memory fragmentation, calls to malloc fail even though available free memory may be greater than the requested size.</p> <p>There are no known workarounds.</p>
CSCee00895	<p>On a Cisco uBR10000 series router, packets switched by PXF are counted as process switched packets for the backhaul interfaces. While this provides accurate information for SNMP and the <b>show interface</b> command it may not accurately reflect the performance of the router as viewed via the <b>show interface switching</b> command. The IP protocol counters displayed by that variant of the show command adds the number of PXF switched packets to the number of process switched packets and may give the impression that packets are being switched by the routing processor instead of the PXF hardware.</p> <p>Workaround: For receive packets, the <b>show pxf cpu statistics diversion</b> command can be used to see how many packets were diverted to the RP per line card. Subtracting that number from the interface's input counter will show if the majority of packets are being PXF switched for a given interval.</p> <p>No such workaround exists for output packets.</p>
CSCee93770	<p>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.</p> <p>Workaround: Hardware Module reset the Protect line card.</p> <p>Alternative workaround: shut/no shut the non-functional interfaces.</p>
CSCef31956	<p>This is a bug to improve reverse arp lookup on the CMTS for modem bringup.</p> <p>There are no known workarounds.</p>

Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCef35392	<p>All Cable Modems on unspecified DS of a Cisco uBR10-MC5X20U card become offline after a Hot Standby Connection-to-Connection Protocol (HCCP) switchover and stay in the “offline” state.</p> <p>A <b>show controller cable x/y/z</b> shows “No MAP buffer” incrementing and the “UCD Count” for each upstream stuck.</p> <p>This issue occurs when conducting HCCP N+1 redundancy with Cisco uBR10-MC5X20U on Cisco IOS Release 12.2(15)BC2b.</p> <p>Workaround: Reset the LC by <b>hw-module subslot x/y reset</b>.</p>
CSCef40864	<p>It is possible that when a cable bundle slave interface is shut/no shut, it cannot repopulate the cable bundle forwarding table with some IGMP static group defined on master interface.</p> <p>There are no known workarounds.</p>
CSCef42977	<p>Under heavy loads (around 500 kpps), the Cisco uBR10000 PXF can stop dequeuing packets from the low priority queues (default data queues).</p> <p>Workaround: The issue can be rectified by a PXF reload (microcode reload pxf).</p>
CSCef43462	<p>Unable to obtain SNMP MIB info correctly after Performance Routing Engine (PRE) switchover, but able to obtain ifDescr correctly. However, some interface info are missing.</p> <p>This issue occurs in PRE redundancy with Cisco uBR10012 Cisco IOS Release 12.2(15)BC2b and 12.2(15)BC2c.</p> <p>Workaround: Reload PRE or enter the <b>cable upstream max-ports</b> command to force the PRE to download the snmpinfo to the cable line card automatically.</p>
CSCef45655	<p>To facilitate understanding the operational condition of a CMTS, the following summary commands have been added to <b>show tech</b> in Cisco IOS Release 12.3BC and later.</p> <p>These commands are generally available from the CLI:</p> <pre>show cable modem summary total show cable modem vendor summary show cable modem mac summary show cable modem rogue show cable qos profile</pre> <p>There are no known workarounds.</p>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCef46191	<p>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.</p> <p>All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.</p> <p>Cisco will make free software available to address this vulnerability.</p> <p>Workarounds, identified below, are available that protect against this vulnerability.</p> <p>The Advisory is available at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet</a></p>
CSCef49769	<p>The 2x8 LC on the Cisco uBR10000 series 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.</p> <p>This can cause box-wide issues as the LC throttles the PXF severely.</p> <p>Workarounds: Reduce load on the affect line card by moving CMs to a different LC. If you have an LCP1 based 2x8 line card, replace with LCP2 Replace 2x8 line card with 5x20 line card.</p>
CSCef52235	<p>A Cisco uBR10000 series router running either Cisco IOS Release 12.2(15)BC2c or 12.2(15)BC1b will run into the following issues when a 2x8 LC is running at 100% CPU:</p> <ol style="list-style-type: none"> <li>1. No telnet access, only the console port works.</li> <li>2. Modems that are online cannot come back online, the get stuck in init(rc).</li> <li>3. Message that is being seen when the CMTS becomes unreachable:  <pre>%C10KEVENTMGR-1-MINOR_FAULT: PXF DMA Full OCQ Wait Error</pre> </li> <li>4. Traffic slowing down for all the line cards, especially the backhaul interfaces.</li> </ol> <p>The issue was seen on a Cisco uBR10000 series router with 16,000 CMs.</p> <p>Workaround: Reduce load on the LC running at 100% CPU.</p> <p>Alternative workaround: Reload the PXF microcode.</p>
CSCef52785	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.2(15)BC2c unexpectedly reloads at boot up.</p> <p>There are no known workarounds.</p>

Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCef53390	<p>The sample rate range is calculated based on the monitoring duration as compared to the previous (STM1.0) constant range of 10 - 30 minutes. The range is calculated as follows:</p> <ul style="list-style-type: none"> <li>• The maximum memory to be used per line card for STM is 10 MBytes.</li> <li>• The maximum number of modems that can be supported is 6000 per line card. Now, per sample memory consumption is 8 bytes hence approximately, the maximum number of samples that can be allowed are <math>10 * 10^6 / (6 * 10^3 * 2 * 8) \sim 100</math>. Hence, given the duration the sample rate would be calculated as duration / 100 = sample rate only if the duration happens to be more than 1440. For monitoring duration less than 1440, the sample rate range would be 10 - 30 minutes.</li> </ul> <p>Hence, with STM 1.0 if someone had the duration as 2 days and the sample rate was 20 minutes, that command would fail when we try to restore that configuration in STM1.1 as now the range would be 28 to 86 minutes. The feature to convert the STM1.0 configuration to STM1.1 was committed through CSCee58978.</p> <p>There are no known workarounds.</p>
CSCef54096	<p>A Cisco uBR10000 series router may unexpectedly reload due to IP INPUT process.</p> <p>There are no known workarounds.</p>
CSCef56071	<p>An enforce-rule configured using SNMP is not effective at the CMTS.</p> <p>The same rule when configured using CLI does not have any issues.</p> <p>There are no known workarounds.</p>
CSCef56516	<p>Signal-to-noise ratio (SNR) values can lower then expected with MC520u card.</p> <p>This issue occurs if virtual connectors 16,17,18,19 are used.</p> <p>There are no known workarounds.</p>
CSCef57375	<p>On an Cisco 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.</p> <p>There are no known workarounds.</p>
CSCef58105	<p>Show cable modem offline does not correctly show the previous state of the modem when going through the provisioning steps.</p> <p>There are no known workarounds.</p>
CSCef59093	<p>A Cisco uBR-MC28U cable interface line card may unexpectedly reload in an Cisco uBR7200 series CMTS running Cisco IOS Release 12.2(15)BC2b.</p> <p>This issue only occurs with MC28U line card. The MC16C line card in the same chassis works correctly.</p> <p>There are no known workarounds.</p>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description																				
CSCef60697	<p>Fix chassis unexpectedly reloads due to ACL processing of fragmented packets. The Cisco uBR10000 series router will crash when the RP processor processes a 0th fragmented packet on an interface that has an ACL attached.</p> <p>This issue occurs when an ACL is attached to an interface &amp; the packet is a 0th fragmented packet.</p> <p>There are no known workarounds.</p>																				
CSCef60926	<p>In a 1.0+ redundant environment, if a switchover is issued using the <b>hccp x switchy</b> command, new downstream dynamic service flows are not established on all new call attempts through the Protect card.</p> <p>There are no known workarounds.</p>																				
CSCef61802	<p>During a Performance Routing Engine (PRE) switchover, the following error message and traceback may appear at the active PRE:</p> <pre>SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 62F70160.</pre> <p>There are no known workarounds.</p>																				
CSCef63012	<p>During an N+1 switchover, the following CPUHOG error message may appear at the PROTECTOR cable line card (CLC) as well at RP:</p> <pre>%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (1200/1160),process = HCCP_DATA_P1.</pre> <p>There are no known workarounds.</p>																				
CSCef64537	<p>The Hot Standby Connection-to-Connection Protocol (HCCP) unlock command causes a CMTS to unexpectedly reload intermittently.</p> <p>This issue occurs when using the HCCP unlock command.</p> <p>There are no known workarounds.</p>																				
CSCef65077	<p>The PRE2 FIB code has been modified so that packets with the PUNT adjacency flag now get a new divert-code of PS_DIVERT_CODE_FIB_RP_PUNT.</p> <p>Packets with the RECEIVE adjacency flag continue to get PS_DIVERT_CODE_FIB_RP_DEST, but the RP_DEST divert-code has now been assigned a priority of 5 (instead of zero). The RP_PUNT divert-code gets a priority of zero. The treatment of GLEAN adjacencies remains the same:</p> <table border="1" data-bbox="613 1417 1315 1570"> <thead> <tr> <th>adjacency flag</th> <th>old div-code</th> <th>old priority</th> <th>new div-code</th> <th>new priority</th> </tr> </thead> <tbody> <tr> <td>GLEAN</td> <td>FIB_RP_GLEAN</td> <td>0</td> <td>FIB_RP_GLEAN</td> <td>0</td> </tr> <tr> <td>PUNT</td> <td>FIB_RP_DEST</td> <td>0</td> <td>FIB_RP_PUNT</td> <td>0</td> </tr> <tr> <td>RECEIVE</td> <td>FIB_RP_DEST</td> <td>0</td> <td>FIB_RP_DEST</td> <td>5</td> </tr> </tbody> </table> <p>SNMP and telnet traffic gets the RECEIVE adjacency flag, and will now be diverted with high priority.</p> <p>This DDTS was created when it was shown that on the PRE2, SNMP and telnet traffic timed-out under congestion conditions. Testing shows that the problem has been fixed. See Test-Results and email-trail attachments.</p> <p>There are no known workarounds.</p>	adjacency flag	old div-code	old priority	new div-code	new priority	GLEAN	FIB_RP_GLEAN	0	FIB_RP_GLEAN	0	PUNT	FIB_RP_DEST	0	FIB_RP_PUNT	0	RECEIVE	FIB_RP_DEST	0	FIB_RP_DEST	5
adjacency flag	old div-code	old priority	new div-code	new priority																	
GLEAN	FIB_RP_GLEAN	0	FIB_RP_GLEAN	0																	
PUNT	FIB_RP_DEST	0	FIB_RP_PUNT	0																	
RECEIVE	FIB_RP_DEST	0	FIB_RP_DEST	5																	

Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCef65495	<p>If the bandwidth command is configured on a cable interface it can cause incorrect bandwidth to be given to the downstream service flows on a Cisco uBR10000 series router.</p> <p>Workaround: Unconfigure <b>bandwidth</b> command from the cable interface.</p>
CSCef68419	<p>A Cisco uBR 10000 series router running Cisco IOS Release 12.2BC images may crash by a Sgtrap exception if an extremely low bandwidth value is specified under a cable interface:</p> <pre>CMD: 'bandwidth 10 ' 12:01:34 Tue Sep 7 2004 Sep 7 09:01:35.359: %SYS-5-CONFIG_I: Configured from console CMD: 'sho cable modem flap</pre> <p>Unexpected exception, CPU signal 5, PC = 0x6012CB08  -Traceback= 6012CB08 6012D65C 603180E0 60318BA0 603063C4 60306878  60315FCC  6050BD68  6050BD4C</p> <p>There are no known workarounds.</p>
CSCef68700	<p>The active PRE2 (Secondary) crashes with Bus Error Exception and System Switched to standby (Primary) PRE2.</p> <p>There are no known workarounds.</p>
CSCef69368	<p>When toaster VTMS receives excessive OCQ flow off from a line card of to-rp link, it can cause severe performance degradation of VTMS or it can lockup the timing wheel causing VTMS not to service any line card.</p> <p>This issue occurs when excessive OCQ flow off from line card e.g in presence of over subscription of link.</p> <p>There are no known workarounds.</p>
CSCef70056	<p>After a CLI switch over, customer premises equipment (CPE) devices on the slave interfaces lose connectivity.</p> <p>Workaround: Reload the CPE device.</p>
CSCef70739	<p>A “MAXMEMORY USED Reached maximum amount of memory allocated for stile” error is displayed at the console and the “Active links” for the <b>show ip nbar resources</b> command will show 4 GB plus.</p> <p>When the NBAR feature is activated, that is, when <b>match protocol protocol-name</b> is included in a policy map, or <b>ip nbar protocol-discovery</b> is applied on an interface, the “MAXMEMORY USED Reached maximum amount of memory allocated for stile” error may appear on the console.</p> <p>Workaround: Perform <b>no ip nbar resources</b> to reset active links back to zero.</p>
CSCef73242	<p>A Cisco uBR series CMTS running Cisco IOS Release 12.2(15)BC2b may not guarantee configured QoS levels on Downstream dynamic Service Flows in Voice over IP (VoIP) networks.</p> <p>This issue can be seen with very high SFIDs (between 32768 and 65535) and when cable modems are provisioned with non-zero active QoS Timeout.</p> <p>Workaround: Increase the bandwidth for Best Effort (BE) flow.</p>

**Table 92**      **Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCef74063	<p>Router may unexpectedly reload under error condition that gate is freed on RP, but not LC, prior to resource being allocated through dsa-req from eMTA. Gate lookup failure on RP causes illegal access to stale gate entry pointer and may unexpectedly reload the RP.</p> <p>This issue does not affect prior release trains before Cisco IOS Release 12.3(9)BC.</p> <p>There are no known workarounds.</p>
CSCef74956	<p>Following a reload of the toaster microcode, there have been cases where it appears as though the output packet count, as reported by “sh int [interface]”, stops incrementing.</p> <p>The “microcode reload pxf” triggers this issue.</p> <p>There are no known workarounds.</p>
CSCef75363	<p>After a N+1 switchover, the ARP entry for customer premises equipment (CPE) devices is 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.</p> <p>Workaround. CPE traffic will recover without any user intervention.</p>
CSCef75566	<p>During LC switchover, the slave interface does not sync over any IGMP Static Group.</p> <p>Workaround: Reconfigure the IGMP static group on master interface.</p>
CSCef77451	<p>After issuing the test crash command the output pauses before printing out the menu options. When this pause occurs, hitting &lt;Enter&gt; allows the menu be printed and the user to select an option.</p> <p>There are no known workarounds.</p>
CSCef77655	<p>When loading a PRE2 image onto a PRE1 card, the boot prompt changes to “invalid image for platform” and is never changed back; even after loading a good image.</p> <p>This issue occurs when loading a PRE2 image onto PRE1 card or vice versa.</p> <p>There are no known workarounds.</p>
CSCef78292	<p>CPUHOG traceback appears on the RP console during switchover.</p> <p>This issue occurs on large-scale systems, &gt;35K CMs, possibly scrypt kiddies.</p> <p>Also, cable bundle has to be configured and switchover has to be configured and performed within this bundle.</p> <p>There are no known workarounds.</p>
CSCef79820	<p>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.</p> <p>This issue occurs in the docsis-mode is tdma-atdma (mix) mode in Cisco IOS Release 12.2(15)BC2a and later releases.</p> <p>Workaround: Use the <b>cable upstream x shutdown</b> and <b>no cable upstream x shutdown</b> commands.</p>

Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCef82436	When we have more than 2K modems ranging on an active interface, the standby LC can reload unexpectedly, while synching those ranged SIDs into its inter-db. There are no known workarounds.
CSCef83385	CPUHOG traceback messages appear on the cable line card (CLC) console during large-scale switchover. This issue occurs with ~39K CMs on Cisco uBR10000 series routers. 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.
CSCef83933	LC HA: N+1 using 520U card will not work after switch over when BPI/PHS and Virtual Interface are configured. There are no known workarounds.
CSCef85824	The router may reload as a result of the following CLI commands: <b>show tech</b> <b>show pxf cpu queue cable interface</b> <b>show cr10k cable interface queue be</b> <b>show cr10k cable interface queue ll</b> <b>show cr10k cable interface queue cir</b> 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.
CSCef87118	In Cisco IOS Release 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	Line card unexpectedly reloads during N+1 switchover. There are no known workarounds.
CSCef94530	If an existing etherchannel member is removed and added back to the etherchannel, the link will not carry traffic. Workaround: Shut down the interface of the link to be removed/added prior to the addition to the etherchannel.
CSCef94945	When the router is coming out of startup and the initial table_id write to toaster memory is performed the write would fail, the toaster was not ready for the write to toaster memory at this time. Code has been added to perform the toaster write when the toaster is available after startup. There are no known workarounds.

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCeg05210	<p>If the CMTS cable arp request filter is configured to filter all arp requests, it appears to not filter at all. In reality, all arp requests are being filtered, but not statistically accounted for.</p> <p>Example config:</p> <pre>interface Cable8/0/0 ... cable arp filter request-send 0 2</pre> <p>Example output:</p> <pre>show cable arp-filter Cable8/0/0 ARP Filter statistics for Cable8/0/0:   Replies Rcvd: 22 total. 0 unfiltered, 0 filtered   Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered   Requests Forwarded: 2000 total. 0 unfiltered, 0 filtered</pre> <p>Note that Requests Forwarded “filtered” count is 0.</p> <p>Note that this is an unusual configuration because if the arp request filter is set to filter all packets, modems will not come online. So this configuration is only used for debug purposes.</p> <p>All versions of CMTS software that support the cable arp filter feature on Cisco IOS Releases 12.2(15)BC2 and 12.3(9)BCa.</p> <p>There are no known workarounds.</p>
CSCeg05586	<p>Voice calls fail on a Cisco uBR10000 series router running Cisco IOS Release 12.3(8.4)BC. Specifically, the downstream dynamic service flow is dropping packets.</p> <p>There are no known workarounds.</p>
CSCeg07988	<p>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.</p> <p>If SNMP set is done, it will show the update Val. It will also update the modulation profile in the CMTS CLI, but the modems will not apply it to the modems.</p> <p>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.</p> <p>This issue occurs on a Cisco uBR10000 series router with a PRE1 and an MC520 card running Cisco IOS Release 12.2(15)BC2b.</p> <p>Workaround: Use the CLI to change the modulation profiles.</p>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCeg12481	<p>DHCP Proxy feature configured on the Cable Modem, is not supported by CMTS. The CMTS is dropping the DHCP OFFER from the DHCP server if the ip address assigned to a customer premises equipment (CPE) does not belong to any directly connected interface.</p> <p>This problem is being triggered by CSCee84392.</p> <p>This message is the one that could be seen if DHCP debug is enabled:</p> <pre>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</pre> <p>There are no known workarounds.</p>
CSCeg14041	<p>A Cisco uBR10000 series router with PRE1-RP processor running Cisco IOS Release 12.2(15)BC2d reloads unexpectedly with a bus error after an interface flapping. The sequence and error message would be seen as follows:</p> <pre>%UBR10000-6-CMOVED: Cable modem &lt;MAC_address&gt; 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</pre> <p>There are no known workarounds.</p>
CSCeg17018	<p>Some single bit ECC errors will unexpectedly reload the 520S-D line card, even though the GT64120 controller can handle single bit ECC errors.</p> <p>There are no known workarounds.</p>
CSCeg23455	<p>The PXF queue allocation fails due to insufficient queue resources, even though there are only small number of queues on the interface.</p> <p>Further investigation found that the problem was caused by stale secondary (dynamic) service flows on the RP.</p> <p>It is unclear what conditions causes this problem, but it is likely to have been induced by Performance Routing Engine (PRE) switchover.</p> <p>Workaround: Clear the cable modems to which the stale service flow belongs.</p>
CSCeg28052	<p>When the MTAs are on the bundle slave interface, there is no call content for CALEA calls for the Cisco uBR10000 series router.</p> <p>Workaround: Configure the MTAs on bundle master or non-bundle interface.</p>
CSCeg30130	<p>In CSCee32618, the user got a traceback following a “No current_if_info” message.</p> <p>There are no known workarounds.</p>
CSCeg30535	<p>CM config files with Min Reserved Traffic Rate set to zero was being handled wrong in the PRE2.</p> <p>This value must be set to a non-zero value else the SF gets no bandwidth at all, resulting in all packets dropped on the DS.</p> <p>There are no known workarounds.</p>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCeg36445	<p>A Cisco Universal Broadband Router may reload unexpectedly as a result of its memory getting corrupted. This will cause a switchover to the standby Performance Routing Engine (PRE).</p> <p>There are no known workarounds.</p>
CSCeg41331	<p>PRE2 punt ISR to handle diverted packets from the pxf engine to the RP processor is not implemented as an inline “C” function. The PRE1 function is implemented as an inline function. That leads to slightly slower performance on PRE2 compared to PRE1.</p> <p>There are no known workarounds.</p>
CSCeg42335	<p>A Cisco uBR10012(Pre1) Broadband Router may experience a packet latency/loss issue on cable interfaces when <b>cable source-verify [dhcp]</b> is configured.</p> <p>This issue occurs on a Cisco uBR10012(Pre1) Broadband Router that runs Cisco IOS Release 12.2(15)BC02 when the cable interfaces have <b>cable source-verify [dhcp]</b> configured. The symptom may occur also in other releases.</p> <p>Workaround: Turn off source verify. Reload the box, shutdown all the cable interfaces (or all the cable bundle master interfaces), and then bring them up one by one. Micro reload pxf switchover.</p>
CSCeg44108	<p>A Cisco uBR 10000 series router may trigger an unexpected PXF processor reload.</p> <p>A large access-list must be applied on a Cable interface. The reload often occurs 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.</p> <p>The router will log the following messages:</p> <pre data-bbox="613 1203 1528 1308">%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</pre> <p>The PXF processor will resume operating, but may unexpectedly reload again in a cycle until the condition has been cleared.</p> <p>The unexpected reload occurs only when a split ACL is in use. Splits in ACLs can be observed with “show pxf cpu access-list security”.</p> <p>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.</p>
CSCeg55961	<p>The entPhysicalName needs to display the type of Performance Routing Engine (PRE) along with the interface name. So, basically it needs to specify whether the interface belongs to the active PRE or the standby PRE.</p> <p>Currently the output displays:</p> <pre data-bbox="613 1696 1101 1717">entPhysicalName.29 = FastEthernet0/0/0</pre> <p>It needs to be changed to:</p> <pre data-bbox="613 1770 1182 1791">entPhysicalName.29 = PRE_X:FastEthernet0/0/0</pre> <p>whereas “X” may be A or B. At any given time either “A” or “B” would be active or standby.</p> <p>There are no known workarounds.</p>

Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCeg56960	<p>The following happens on the line card when a Performance Routing Engine (PRE) switchover happens:</p> <pre>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</pre> <p>This issue occurs if all ipc traffic is not properly cleared.</p> <p>There are no known workarounds.</p>
CSCeg58842	<p>This problem should only pop up if flow-aggregation of type prefix is enabled (the CLI is “ip flow-aggregation cache prefix”).</p> <p>There are no known workarounds.</p>
CSCeg71365	<p>A CM may stop responding if both BPI and LoadBalancing are configured and a DOCSIS UCC-request is used to move it from one upstream to another. The problem is specific to the MC520 line card and only affects DOCSIS 1.1 modems which support the ranging technique TLV in the UCC-request.</p> <p>The UCC-request can be generated as part of a normal load balancing operation or in response to the either the <b>TEST CABLE LOAD</b> or <b>TEST CABLE UCC</b> commands.</p> <p>Workaround: This problem does not always occur. However, if the modem becomes unreachable following an upstream channel, change use the clear cable modem command to delete it from the CM database.</p>

Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCeg71922	<p>One or more line 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).</p> <p>A crashinfo file is left on the line card with CPU Hog messages from the “CMTS Mac Timer” process, followed by a watchdog reset.</p> <p>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.</p> <p>The conditions for this issue are:</p> <ul style="list-style-type: none"> <li>• Line card must have been up for 49 days</li> <li>• Service flows must have a non-zero activity timer</li> <li>• PacketCable configurations are more vulnerable than pure data configurations because voice service flows typically use activity timers.</li> </ul> <p>This issue has been observed on uBR10k 520 line cards, but any cable configuration, including 7246, that uses service flow activity timers is vulnerable.</p> <p>Workarounds: The following are possible workarounds:</p> <ol style="list-style-type: none"> <li>1. Set the service flow activity timer to zero a few hours before the clock will rollover. Reenable the activity timer after the rollover.</li> <li>2. Check the uptime of the cards in the system, schedule a card reload prior to the rollover.</li> <li>3. If N+1 is configured: switch a card to the redundant card, reload the Working card and then revert. Repeat for all cards approaching the 49 day rollover point.</li> </ol> <p> <b>Note</b> The up time of a line card can be seen with the <b>show diag</b> command.</p>
CSCeg78636	<p>A file name or file names that are shown by the <b>dir</b> command may not be displayed by the <b>show</b> command.</p> <p>This issue will only occurs on PCMCIA ata-disk or Compact Flash devices.</p> <p>If a file exists that is 0 bytes in size, it will cause one file to not be displayed when a <b>show</b> is performed on the device.</p> <p>The problem may also occur if the PCMCIA ata-disk card is given a soft label while it is in a Microsoft Windows PC as soft labels have a 0 byte size on the PCMCIA ata-disk.</p> <p>Workaround: Do not create a soft label in a Microsoft Windows PC for the PCMCIA ata-disk card. If such a label exists, use a Microsoft Windows PC to remove the label.</p> <p>If any file of size 0 bytes is displayed by the <b>dir</b> command on the device delete the file.</p>
CSCeg80463	<p>This issue is not reproducible.</p> <p>There are no known workarounds.</p>

Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)

DDTS ID Number	Description
CSCeh00967	<p>A Cisco uBR10000 series router running Cisco IOS Release 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”</p> <p>This issue occurs with cable spectrum-group configured on different cable interfaces, and if the total number of interface on the system needs exceeds 144</p> <p>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”.</p>
CSCeh01845	<p>Poor and irregular p performance results with 64 and 512-byte packet sizes on 12.3(9a)BC1 pre-fcs image.</p> <p>Workaround: Disable fragmentation by configuring “no cable upstream n fragmentation”.</p>
CSCeh18068	<p>The cable upstream power-level is set 0 dbmV after reload.</p> <p>This issue occurs when the configure cable upstream power-level is above 23 dbmV on upstream</p> <p>Workaround: Reconfigure <b>cable upstream power-level</b>.</p>
CSCeh22118	<p>Modems connected to a JIB based distributed line card, such as the MC520u or MC28u, come online and enter the online(pt) state as seen in the <b>show cable modem</b> command display. Shortly after that, all modems connected to the downstream interface go offline and stay offline until the line card is reset. A shutdown/no-shutdown command sequence will not clear the problem. The module must be OIR'd by physically removing it or by using either the <b>microcode reload</b> command on the VXR7246 or the <b>w-module slot x reset</b> command on the Cisco uBR10000 series router.</p> <p>This issue occurs when the modem's DOCSIS configuration file enables BPI and provisions a secondary upstream service flow. If the secondary flow is simply provisioned and not admitted, the downstream interface becomes blocked.</p> <p>Workaround: If a secondary upstream is to be provisioned but not activated, it must use a QoS parameter set type value of 0x03. This allows the service flow to be provisioned and admitted without being activated. When the flow is admitted, it is assigned a Service ID and the presence of the SID value avoids the problem.</p>
CSCeh27333	<p>The <b>cable service class 200</b> command is accepted by the CLI. This creates service class with a index but no name. In the running config, this shows up as <b>cable service class 200 name</b>, which is an incomplete command.</p> <p>Workaround: Enter name with the <b>cable service class</b> command.</p>
CSCeh37712	<p>This fix enables the LCHUNG process on the Cisco uBR10000 RP. This process will power cycle any hung cable line card. There is an exec command <b>auto-clc-hang-reset onloff</b> which can disable or enable the polling. The default will be enable.</p> <p>There are no known workarounds.</p>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCeh42526	<p>The LCHUNG process on Cisco uBR10000 series router does 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.</p> <p>There are no known workarounds.</p>
CSCeh42853	<p>A Cisco uBR10000 PRE2 may unexpectedly reload due to a race condition at bootup.</p> <p>There are no known workarounds.</p>
CSCeh57367	<p>Some CF functions do not correctly interpret flows where the traffic from one side has stopped because the other side has been placed on hold. The CMTS can change its behavior slightly to help them correctly replay these streams.</p> <p>There are no known workarounds.</p>
CSCeh69053	<p>GET SNMPv2-MIB:sysUpTime.0 fails with SNMPv1</p> <p>There are no known workarounds.</p>
CSCei00243	<p>In an MPLS-VPN environment, the LAN side IP address of customer premises equipment (CPE) router cannot be reached from a remote CMTS, and business customers on the LAN do not have connectivity.</p> <p>Workaround: Create a new loopback interface in a “TEST” vrf, routing traffic for the CPE “Lan” subnet to that new loopback interface, and then having another static route in the “TEST” vrf routing table that points back to the real location of the network.</p> <p>For example:</p> <p>In vrf “SP2” with CPE Router “WAN” IP 192.168.31.10 and “LAN” subnet is 99.99.99.0, instead of using the following static route on the Cisco uBR10000 series router:</p> <pre data-bbox="613 1266 1328 1287">ip route vrf ISP2 99.99.99.0 255.255.255.0 192.168.31.10</pre> <p>You would instead apply:</p> <pre data-bbox="613 1339 1474 1728">ip vrf TEST          ! The new "temporary" vrf  rd 9999:9999 ! interface Loopback9999 ! The new "temporary" loopback interface  ip vrf forwarding TEST  ip address 5.6.7.8 255.255.255.255 ! ! ip route vrf ISP2 99.99.99.0 255.255.255.0 Loopback9999 5.6.7.8 ! The IP address of Loopback9999 ! ip route vrf TEST 99.99.99.0 255.255.255.0 Bundle 1.2 192.168.31.10 ! Replace Bundle 1.2 with the appropriate subinterface !</pre> <p>The main drawback of this workaround is that it would be hard to scale for more than a few such network numbers.</p>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCei10160	<p>Encryption keys are not created. As a result, multicast traffic does not get encrypted.</p> <p>This issue occurs when static igmp groups are present on bundle interface CMs are BPI+ capable.</p> <p>There are no known workarounds.</p>
CSCin80987	<p>In a HA enabled CMTS, if a “clear cable modem” CLI is invoked and the CMTS any time later performs a Performance Routing Engine (PRE) switchover and QoS profile reference counts on the standby PRE will be completely wrong.</p> <p>This causes QoS profile deletion/addition behavior to be totally wrong after the switchover for all times to come.</p> <p>There are no known workarounds.</p>
CSCin82115	<p>If the UGS DOCSIS.1 config file is provisioned to the toshiba modem with BPI+ enabled traffic may get stuck after switchover.</p> <p>There are no known workarounds.</p>
CSCin82407	<p>Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.</p> <p>Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.</p> <p>This advisory will be posted to <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050406-xauth">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050406-xauth</a></p>
CSCin84603	<p>Executing the <b>no debug all</b> command or the <b>undebug all</b> can result in the following error message, along with a traceback:</p> <pre>%SCHED-7-WATCH: Attempt to enqueue uninitialized watched queue (address 0).</pre> <p>This problem occurs only when an SRP/OC-12 line card is installed in the CMTS.</p> <p>There are no known workarounds.</p>
CSCin87617	<p>CMTS unexpectedly reloads while the modem is trying to get authenticated with the Authentication, Authorization, and Accounting (AAA) server.</p> <p>Cable privacy authenticate-modem CLI was configured and the unexpected reload occurs only if debug radius is enabled in CMTS. This is easily reproducible with MC28C as well as MC520S testbeds.</p> <p>This issue occurs under the following and is verified to exist in Cisco IOS Releases 12.2(15)BC2e and 12.3(9a)BC1:</p> <pre>debug radius cable privacy authenticate-modem</pre> <p>Workaround: Do NOT attempt to debug radius while using “cable privacy authenticate-modem”.</p>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsa41720	<p>A Cisco uBR10000 CMTS router with PRE1 may unexpectedly reloads while unconfiguring routing protocols or changing or removing the ip address on interface.</p> <p>There are no known workarounds.</p>
CSCsa42887	<p>Cable modems under the Bundle Mater fail init(o) when the bundle is number 1.</p> <p>Workaround: Number the bundle &gt; 1.</p>
CSCsa44591	<p>Tacacs TCP session between router and ACS hangs with the single connection option.</p> <p>This issue occurs on a Cisco uBR router running Cisco IOS Release 12.3(9a)BC.</p> <p>Workaround: Remove the “single-connection” option with the Tacacs+ config. When this issue occurs, turn off and turn on the “single connect” option.</p>
CSCsa47427	<p>With dynamic secret enabled, if ALL conditions described below are true, modems may get stuck in init(o) state and fail to register.</p> <p>The conditions are:</p> <ol style="list-style-type: none"> <li>1. Each modem gets its own config file (for e.g. as when BACC is used for provisioning).</li> <li>2. The CM config files are large (greater an 1024 bytes in size).</li> <li>3. Large number are trying to connect to the CMTS.</li> <li>4. The RP CPU is high (close to 100%).</li> </ol> <p>Workaround: The only workaround is to reduce the number of modems trying to connect to the CMTS at the same time. This includes increasing insertion interval and ranging backoffs, shutting down interfaces or upstreams.</p>
CSCsa48550	<p>Multicast flows are classified to a default flow. This fix will increase the priority and queue depth of the default queue, thus assuring higher quality for mcast flows.</p> <p>There are no known workarounds.</p>
CSCsa50053	<p>Cable intercept might stop sending copy of downstream packets to the collection server. Only upstream packets appear on the collection server.</p> <p>There are no known workarounds.</p>
CSCsa50929	<p>The Fix for CSCsa48673 will cause US Load Balancing to not decrement the Pending count.</p> <p>There are no known workarounds.</p>
CSCsa53912	<p>You cannot log on when a TACACS+ server is used for authentication. You get a message that authentication fails and you are asked again to enter your user name.</p> <p>This issue occurs when you make a Telnet connection to a router that is configured for TACACS+ after you have entered you user name and your TACACS password.</p> <p>Workaround: Configure the TACACS+ single connection option by entering the <b>tacacs-server host <i>host-name</i> single-connection</b> command.</p>

**Table 92** *Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsa54614	<p>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. But 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.</p>
CSCsa59295	<p>On the Cisco uBR10000 series platform, the Performance Routing Engine (PRE) unexpectedly reloads. The unexpected reloads reported may contain: System returned to ROM by bus error at PC 0x&lt;varies&gt;, address 0xB0D0B5D at (time)...</p> <p>These issues may occur under stress situations with large numbers of unstable cable modems (modems do not stay online and cause their arp entries to be deleted), and intensive SNMP polling of the entire cable modem database, the Cisco uBR10000 series router may experience PRE failovers. In particular, querying the atEntry table will cause the problem. The fault has been observed in Cisco IOS Releases 12.2(15)BC2d, BC2e, BC2f, and 12.3(9a)BC, 12.3(9a)BC2. A specific testbed was able to reproduce this crash about once every 12-36 hours. Workaround: Disable intensive SNMP polling. Improve modem stability. Utilize redundant PREs, and the system will remain operational. The redundant PRE will take over successfully, the failed PRE will recover, and be available before the redundant PRE fails again.</p>
CSCsa69764	<p>SAMIS is enabled in Streaming Mode. If, for some reason, the Cisco uBR router was unable to send data to the server in the middle of streaming metering status is “write-error”; but when the destination server recovers, the cable metering status does not change and no more SAMIS information is exported to the server. There are no known workarounds.</p>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCsa69875	<p>With arp reply filter enabled, a modem will show as “online” from “show cable modem” but may not have an arp entry. <b>show ip arp modem ip addr</b> will be empty.</p> <p>This issue occurs when the cable interface command <b>cable arp filter reply-accept packets time window</b> is present and virus activity is high on the CMTS.</p> <p>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:</p> <pre>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</pre> <p>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.</p> <p>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:</p> <p><a href="http://homesupport.cisco.com/en-us/support/linksys">http://homesupport.cisco.com/en-us/support/linksys</a></p> <p>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.</p>
CSCsa71054	<p>When trying to change the fixed frequency to the frequency from non-shared spectrum-group with 40 spectrum-group used in a Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC1, the port was not assign the frequency from non-shared-spectrum-group.</p> <p>Before with the fixed image, cable upstream 2 frequency 32000000. After, with non-shared spectrum-group:</p> <pre>Router(config-if)#cab up 2 spec 1 Router(config-if)#^Z Router#show cab spec 1 Group Frequency      Upstream      Weekly Scheduled      Power Shared No.  Band              Port          Availability          Level Spectrum       (Mhz)                From Time:    To Time: (dBmV) 1   Unassigned      Cable6/1/2    U2</pre> <p>Workaround One: Avoid changing an upstream from a fixed frequency to the spectrum group, which has the same fixed frequency as its first one.</p> <p>Workaround Two: Perform “cable up x shut” and then “no cable up x shut” if this issue occurs.</p>
CSCsa74636	<p>When a file in CMTS flash device is used as the CM config file, or when an IOS generated config file is used for provisioning, modems will fail to register.</p> <p>Workaround: Use external TFTP server/file.</p>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCsa76715	<p>Frequent SNMP queries of the Cisco uBR10000 arp table by ipNetToMediaTable or atEntry will result in high CPU usage by the SNMP ENGINE process, upwards to 80%.</p> <p>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.</p> <p>This issue occurs on 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.</p> <p>Although SNMP will usually appear to use high CPU, this problem was made worse on the Cisco IOS Release 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 Cisco IOS Release 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.</p> <p>Workaround: The following are possible workarounds:</p> <ol style="list-style-type: none"> <li>1. If an extreme problem, turn off querying. If snmp servers can't be isolated, setup an ACL on port 161.</li> <li>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.</li> <li>3. Exclude the ipNetToMediaTable from querying. The following config will achieve this: <pre>snmp-server view noarp ipNetToMediaEntry excluded snmp-server view noarp iso include snmp-server community public view noarp ro.</pre>                     The impact of 3 is that there will be no results returned to the tool.                 </li> <li>4. Exclude 3 of the 4 subtables of ipNetToMediaTable. This will cut the querytime by 75%: <pre>ipNetToMediaTable is comprised of 4 tables: ipNetToMediaIfIndex      aka ipNetToMediaEntry.1 ipNetToMediaPhysAddress aka ipNetToMediaEntry.2 ipNetToMediaNetAddress  aka ipNetToMediaEntry.3 ipNetToMediaType        aka ipNetToMediaEntry.4</pre> </li> </ol>

**Table 92 Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)**

DDTS ID Number	Description
CSCsa86851	<p>Intercept does not work on PRE1 when using sub-interface.</p> <p>The sub-interface needs to be used:</p> <p>1- test without bundle without sub-intf ===&gt; ok</p> <p>2- test with bundle without sub-intf =====&gt; ok</p> <p>3- test with bundle with sub-intf ======&gt; FAIL</p> <p>There are no known workarounds.</p>
CSCsb00255	<p>The active Performance Routing Engine (PRE) suddenly stops seeing any of the line cards of the chassis. The ones that are seen, are seen via de SH CONTROLLERS in a bad state:</p> <pre>Sh diag sees nothing but the PREs: Router#sh diag sum Slot A: Primary PRE2-RP card Slot B: Secondary PRE2-RP card Sh controllers sees the cards in bad stated (slot1 not even seen): Router#sh controllers ..... ..... Interface GigabitEthernet4/0/0(idb 0x638B1EB4) Hardware is Half-height Gigabit Ethernet MAC Controller - Not initialized Interface GigabitEthernet7/0/0(idb 0x208370E4) Hardware is Gigabit Ethernet MAC Controller - Not initialized Interface GigabitEthernet8/0/0(idb 0x638BBC40) Hardware is Gigabit Ethernet MAC Controller - Not initialized Workaround: Reload any of the cards.</pre>
CSCsb01435	<p>While trying to configure frequency stacking on C8/1, CMTS toggles configuration of US port so that the last US configured for the shared port is the only US enabled; and the 1st US configured for the same port is disabled.</p> <p>There are no known workarounds.</p>
CSCsb02139	<p>Poor performance in cable modem best effort service flows in the downstream direction.</p> <p>This issue may occur when the Cable interface default queue has some amount of traffic. The more the traffic in default queue, the poorer the performance in BE queues. The default queue is usually used for downstream multicast traffic.</p> <p>There are no known workarounds.</p>
CSCsb05532	<p>The cable line card of the Cisco uBR10000 series router unexpectedly reloads and temporary disconnects every user connected to that cable line card.</p> <p>This issue is exactly similar to the defect mentioned as DDTS # CSCeg14041, but the trigger which was causing the issue is different.</p> <p>Workaround: The unexpected reload was due to the stale flap pointer pointing to a freed chunk memory. It is recommended not to issue “clear cable flap-list all”.</p>

**Table 92** *Resolved Caveats for Cisco IOS Release 12.3(13a)BC (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb06850	<p>After resetting a Protect line card of a Cisco uBR10000 series router with either a OIR or hw-module reset, it was possible to immediately switchover a Working line card to the Protect line card before the Protect line card was fully operational. After switchover of Working line card to Protect line card, all modems would disappear.</p> <p>Workaround: After OIR or hw-module reset of Protect line card, wait until the Protect line card is in a up/down state and all resync timers have elapsed.</p>
CSCsb07065	<p>Unable to configure any of the MQC queueing commands: bandwidth, priority or queueing. CLI simply returns without any error message.</p> <p>This issue occurs when bandwidth, priority or shape commands are typed in for IOS MQC policy-map. Nothing happens... no configuration is created and no error message is printed to the console.</p> <p>There are no known workarounds.</p>
CSCsb11124	<p>The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.</p> <p>Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.</p> <p>Cisco has published a Security Advisory on this issue; it is available at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060118-sgbp">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060118-sgbp</a></p>
CSCsb16998	<p>XML formatting IPDR record is incorrect (e.g: variable Octetspassed is 32-bits long and it should be 64-bits).</p> <p>This issue occurs when using Usage billing feature introduce in 12.3BC train.</p> <p>There are no known workarounds.</p>

## Open Caveats for Release 12.3(9a)BC9

This section documents possible unexpected behavior by Cisco IOS Release 12.3(9a)BC9 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(9a)BC9.

## Resolved Caveats for Release 12.3(9a)BC9

Table 93 lists only severity 1 and 2 caveats and select severity 3 caveats for the Cisco IOS Release 12.3(9a)BC9.

**Table 93**      *Resolved Caveats for Cisco IOS Release 12.3(9a)BC9*

DDTS ID Number	Description
CSCek03346	Late Voice packets are observed to be further delayed, causing voice quality degradation.  There are no known workarounds.
CSCek06198	Voice flows are shaped to their maximum configured bandwidth. This may shape voice packets arriving in a burst and cause voice quality degradation.  There are no known workarounds.
CSCsc55518	PRE2 unexpectedly reloads with the following error in the reload info:  PXF DMA Error - End of Descriptor Before Cmd Byte Length Exhausted There are no known workarounds.

## Open Caveats for Release 12.3(9a)BC8

This section documents possible unexpected behavior by Cisco IOS Release 12.3(9a)BC8 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(9a)BC8.

## Resolved Caveats for Release 12.3(9a)BC8

Table 94 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(9a)BC8.

**Table 94** Resolved Caveats for Cisco IOS Release 12.3(9a)BC8

DDTS ID Number	Description
CSCef28979	<p>If the host IP address is changed after the CM is online, the host IP address is not synched to the standby Performance Routing Engine (PRE) or Protect LC.</p> <p>This would cause delays in traffic recovery after a PRE or LC switchover.</p> <p>There are no known workarounds.</p>
CSCef67682	<p>Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.</p> <p>The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:</p> <pre>interface Ethernet0/0   ipv6 traffic-filter nofragments in ! ipv6 access-list nofragments   deny ipv6 any &lt;my address1&gt; undetermined-transport   deny ipv6 any &lt;my address2&gt; fragments   permit ipv6 any any</pre> <p>This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.</p> <p>This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.</p> <p>We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-IOS-IPv6">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-IOS-IPv6</a> contain fixes for this issue.</p>
CSCeh18068	<p>The cable upstream power-level is set 0 dbmV after reload.</p> <p>This issue occurs when the configure cable upstream power-level is above 23 dbmV on upstream</p> <p>Workaround: Reconfigure <b>cable upstream power-level</b>.</p>
CSCeh64171	<p>After a Performance Routing Engine (PRE) switchover, the cable qos profile created by CM lost is found. Even after a <b>clear cable modem reset</b> is performed to let cable modem re-register.</p> <p>This issue occurs on PRE switchover.</p> <p>Workaround: <b>clear cable modem all reset</b> can get the qos profile back.</p>

**Table 94 Resolved Caveats for Cisco IOS Release 12.3(9a)BC8 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCei04362	<p>Excessive UCD messages are sent for several minutes when upstream is coming up, possibly at a rate of 4ms interval.</p> <p>This issue occurs in a N+1 configuration when standby becomes active.</p> <p>There are no known workarounds.</p>
CSCsa86851	<p>Intercept does not work on PRE1 when using sub-interface.</p> <p>The sub-interface needs to be used:</p> <p>1- test without bundle without sub-intf ==&gt; ok</p> <p>2- test with bundle without sub-intf =====&gt; ok</p> <p>3- test with bundle with sub-intf =====&gt; FAIL</p> <p>There are no known workarounds.</p>
CSCsb00730	<p>Polling docsIfSigQSignalNoise to graph and trap on signal-to-noise ratio (SNR) changes.</p> <p>When zero modems are online, this Mib still has an SNR value in it, even though the show controllers for the upstream port does not.</p> <p>There are no known workarounds.</p>
CSCsb05747	<p>FLAP-LIST is not aging properly in 12.3BC.</p> <p>There are no known workarounds.</p>
CSCsb06850	<p>After resetting a Protect line card of a Cisco uBR10000 series router with either a OIR or hw-module reset, it was possible to immediately switchover a Working line card to the Protect line card before the Protect line card was fully operational. After switchover of Working line card to Protect line card, all modems would disappear.</p> <p>Workaround: After OIR or hw-module reset of Protect line card, wait until the Protect line card is in a up/down state and all resync timers have elapsed.</p>
CSCsb16998	<p>XML formatting IPDR record is incorrect (e.g: variable Octetspassed is 32-bits long and it should be 64-bits).</p> <p>This issue occurs when using Usage billing feature introduce in 12.3BC train.</p> <p>There are no known workarounds.</p>
CSCsb25918	<p>On the MC520s card, signal-to-noise ratio (SNR) values may drop on a upstream causing modems to drop offline. They are running 16 QAM on the upstream.</p> <p>This issue occurs on a Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC1 with multiple MC520s cards. Switching modulation from 16-QAM to QPSK and back restored the SNR levels</p> <p>The Init Mtn Slots were increasing. Utilization on the upstreams did not differ.</p> <p>Workaround: Disable eq-coefficient, change modulation to qpsk, revert back to 16qam and re-enable eq-coefficient.</p>

Table 94 Resolved Caveats for Cisco IOS Release 12.3(9a)BC8 (continued)

DDTS ID Number	Description
CSCsb42361	<p>A Cisco uBR10000 series CMTS may suffer from high CPU in the IP Background process after adding a secondary IP address to a cable or bundle interface.</p> <p>The issue may occur when the number of ARP entries on the interface being configured is in the order of tens of thousands.</p> <p>The number of ARP entries on each interface may be approximately gauged with the <b>show adjacency summary</b> command.</p> <p>Workaround: Ensure that secondary IP addresses are added during a maintenance window.</p> <p>Alternative workaround: Segment the CMTS into small cable interface bundle groups or to use separate subinterfaces so that a lower number of modems and Customer Premise Equipment ARP entries are linked to each subinterface.</p>
CSCsb42820	<p>5x20 line card is hanging in the “check_flap_list” function (%LCINFO-4-LCHUNG) causing a “power cycle” (%UBR10K-1-POWCYCLE).</p> <p>Workaround: Turn off all debugs, or excessive SNMP management of the system, to reduce the size of the flap list to 4000, and change the power-adjustment threshold to 4-6 dB.</p> <p>Alternative workaround: Enter “no logging console guaranteed” on RP and each line card.</p>
CSCsb63551	<p>When examining the local CMTS uBR100012, the router log the following messages:</p> <pre>%AMDP2_FE-6-EXCESSCOLL</pre> <p>This issue can occur under normal operating conditions and with light load. This fix will correct these errors.</p> <p>There are no known workarounds.</p>
CSCsb74136	<p>An unexpected reload will occur when using old Flash Memory and old-style PCMCIA cards like slot0: and slot1: with a small value for the <b>cable sflog</b> command.</p> <p>It is advised that, while using SAMIS, to use newer ATA style PCMCIA cards. Also, the recommended value for the <b>sflog</b> command is as below to obtain deleted service flows. If other values are used, sflog file might need to be created in the filesystem and with slot0: and slot1: being used for the sflog file, the unexpected reload might occur:</p> <pre>cable sflog max-entry 40000 entry-duration 86400</pre> <p>Workarounds: Use <b>cable sflog max-entry 40000 entry-duration 86400</b> to collect the deleted service flow information in SAMIS.</p> <p>Alternative workaround: Use newer ATA style flash cards like disk0:, disk1:</p>
CSCsb76667	<p>GE link flap with TLS (Transparent LAN Service) after N+1 switchover, so end-to-end TLS traffic fail for a few seconds.</p> <p>This issue occurs on Cisco IOS Releases 12.3(9a)BC6 and 12.3(13a)BC and configured TLS and N+1 environment.</p> <p>There are no known workarounds.</p>

**Table 94 Resolved Caveats for Cisco IOS Release 12.3(9a)BC8 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb86672	Cable modems are online but the MTA is not getting IPs. Workaround: Microcode reload pxf.
CSCsb99726	The Cisco router may not be able to utilize the full DS bandwidth on a 520 line card.  This issue occurs when multiple BE service flows try to utilize the full DS bandwidth on a 520 line card.  There are no known workarounds.
CSCsc02416	A Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC6 experiences the following bus error:  System returned to ROM by bus error at PC 0x602BF6E4, address 0x4824 This issue occurs on a Cisco uBR10000 series router running a PRE1 with MC28c &MC520u cards and 15,000 attached devices.  Workaround: Do not use the <b>cable modem mac addr access-group access group number</b> command on the Cisco uBR10000 series router. This command is not supported on the Cisco uBR10000 series router.
CSCsc06630	Executing the <b>hw-module subslot slot/subslot reset</b> command generates non-blocking request and destination port tracebacks:  *Oct 4 12:17:56.784: %REQGRP-3-SYSCALL: System call for command 6 (slot8/0) : Nonblocking request failed (Cause: timeout) -Traceback= 60378C84 606BFC84 606C226C 606C290C 606C3100 *Oct 4 12:18:02.368: %IPC-5-INVALID: Invalid dest port=0x0 -Traceback= 606C0508 606CC39C 606CC22C 606CC4A0 6067BBCC 6067C0D8 6067C59C This issue occurs when the user resets a line card using either the <b>hw-module subslot reset</b> or <b>hw-module slot reset</b> command.  There are no known workarounds.
CSCsc07695	Unable to ping PC-to-PC under cable modem with TLS setting.  This issue is seen on Cisco IOS Release 12.3(9a)BC7 with TLS setting and occurs if the TLS setting is read from startup-config. However, there is no problem when setting it after booting.  Workaround: Reset the <b>cable dot1q-vc-map</b> command.

## Open Caveats for Release 12.3(9a)BC7

This section documents possible unexpected behavior by Cisco IOS Release 12.3(9a)BC7 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(9a)BC7.

## Resolved Caveats for Release 12.3(9a)BC7

Table 95 lists only severity 1 and 2 caveats and select severity 3 caveats for the Cisco IOS Release 12.3(9a)BC7.

**Table 95** Resolved Caveats for Cisco IOS Release 12.3(9a)BC7

DDTS ID Number	Description
CSCee45312	<p>Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.</p> <p>Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.</p> <p>Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.</p> <p>Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.</p> <p>More details can be found in the security advisory which posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050629-aaa">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050629-aaa</a></p>
CSCee82448	<p>A Cisco AS5800 Access Server may send ALIGN-3-SPURIOUS and SSSMGR-3-NULL_INFO_STRING messages in the log.</p> <p>This issue was observed on the Cisco IOS Release 12.3(9.4) interim version.</p> <p>Normal functionality is not influenced by the problem.</p> <p>There are no known workarounds.</p>
CSCeg71365	<p>A CM may stop responding if both BPI and Load Balancing are configured and a DOCSIS UCC-request is used to move it from one upstream to another. This issue is specific to the MC520 line card and only affects DOCSIS 1.1 modems which support the ranging technique TLV in the UCC-request.</p> <p>The UCC-request can be generated as part of a normal load balancing operation or in response to the either the <b>TEST CABLE LOAD</b> or <b>TEST CABLE UCC</b> commands.</p> <p>Workaround: This issue does not always occur, but if the modem becomes unreachable following an upstream channel change; use the <b>clear cable modem</b> command to delete it from the CM database.</p>

**Table 95** *Resolved Caveats for Cisco IOS Release 12.3(9a)BC7 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCeg74394	<p>The primary and backup FE or GE interfaces go into admin shutdown after a reload.</p> <p>While the router is coming backup after a reload, the console will display ethernet coming up and then going down, followed by a “shutdown” noticed under the configuration for both interfaces.</p> <p>This issue only occurs if a higher number FE or GE interface, such as FE0/3 or GE0/3, is configured as primary while a lower number interface, such as FE 0/2 or GE0/2, is configured as backup.</p> <p>This does not occur when the situation is reverse: when a lower number ethernet configured as primary and a higher number ethernet configured as backup.</p> <p>Also, one of the ethernet interfaces will loose its configured IP address and will be “no ip address” instead in the interface configuration.</p> <p>There are no known workarounds.</p>
CSCeg84212	<p>Router may reload by itself due to bus error.</p> <p>This issue only occurs on PRE1 cards in a Cisco uBR10000 router.</p> <p>There are no known workarounds.</p>
CSCeh00476	<p>After a N+1 switchover, the DOCSIS UCD count may be temporarily incorrect. Some brands of modems may go offline.</p> <p>There are no known workarounds.</p>
CSCeh11129	<p>With a high modem count, the Protect line card may report memory allocation errors after a Performance Routing Engine (PRE) switch over.</p> <p>There are no known workarounds.</p>
CSCeh13489	<p>A router may reset its Border Gateway Protocol (BGP) session.</p> <p>This issue occurs when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.</p> <p>Workaround: Configure the <b>bgp maxas limit</b> command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.</p>
CSCeh18798	<p>The CMTS may report a Process Thashing error during modem registration.</p> <p>There are no known workarounds.</p>

Table 95 Resolved Caveats for Cisco IOS Release 12.3(9a)BC7 (continued)

DDTS ID Number	Description
CSCeh22118	<p>Modems connected to a JIB based distributed line card, such as the MC520u or MC28u, come online and enter the online(pt) state as seen in the <b>show cable modem</b> command display. Shortly after that, all modems connected to the downstream interface go offline and stay offline until the line card is reset.</p> <p>A <b>shutdown/no-shutdown</b> command sequence will not clear the problem. The module must be OIR'd by physically removing it or by using either the <b>microcode reload</b> command on the VXR7246, or the <b>hw-module slot x reset</b> command on the Cisco uBR10000 series router.</p> <p>This issue occurs when the modem's DOCSIS configuration file enables BPI and provisions a secondary upstream service flow. If the secondary flow is simply provisioned and not admitted, the downstream interface becomes blocked.</p> <p>Workaround: If a secondary upstream is to be provisioned, but not activated, it must use a QoS parameter set type value of 0x03. This allows the service flow to be provisioned and admitted without being activated.</p> <p>When the flow is admitted, it is assigned a Service ID and the presence of the SID value avoids the problem.</p>
CSCeh66396	<p>On a Cisco uBR10012(Pre1), when the feature "ip verify unicast reverse-path" is configured on sub-interfaces (cable and non-cable interfaces), the feature is not enabled until the router is reloaded or when pxf reload is executed.</p> <p>This issue occurs in the 12.3(9a)BC, BC1, BC2, and BC3 releases. The issue only occurs when "ip verify unicast reverse-path" is configured on a sub-interface while the router is running IOS.</p> <p>Workaround: Execute PXF reload, or reload the router with the "ip verify unicast reverse-path" feature in the start-up config file.</p>
CSCei03655	<p>911 calls will get rejected if no single existing normal voice call can be freed to fit 911.</p> <p>Workaround: Ensure that normal voice calls for QOS parameters can fit 911.</p>
CSCei25282	<p>The line cards may report a keepalive error and unexpectedly reloads.</p> <p>There are no known workarounds.</p>
CSCei61732	<p>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.</p> <p>Cisco has made free software available that includes the additional integrity checks for affected customers.</p> <p>This advisory is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-timers">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051102-timers</a>.</p>

**Table 95** *Resolved Caveats for Cisco IOS Release 12.3(9a)BC7 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCei73998	<p>DS secondary SF is not removed from the standby Performance Routing Engine (PRE) if the SF is deleted when it is in the reserved state. The SF is in the reserved state when it is created for a PC voice call and the call is put on hold.</p> <p>This issue occurs when a PC voice call is put on hold and then the call is terminated while on hold.</p> <p>There are no known workarounds.</p>
CSCei83154	<p>The OIR-compatibility feature is disabled if a secondary Performance Routing Engine (PRE) is installed.</p> <p>The presence of a secondary PRE in standby mode disables the OIR-compatibility setting.</p> <p>Workaround: Shutdown the secondary PRE before upgrading from an MC520S to an MC520u.</p>
CSCsa50053	<p>Cable intercept may stop sending copy of downstream packets to the collection server. Only upstream packets appear on the collection server.</p> <p>There are no known workarounds.</p>
CSCsa54608	<p>The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.</p> <p>Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.</p> <p>Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.</p> <p>Only devices running certain versions of Cisco IOS are affected.</p> <p>Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.</p> <p>This advisory will be posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050907-auth_proxy">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050907-auth_proxy</a></p>

Table 95 Resolved Caveats for Cisco IOS Release 12.3(9a)BC7 (continued)

DDTS ID Number	Description
CSCsa76766	<p>The command line interface on a Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC2 becomes sluggish, if the user enters the following command:</p> <pre>rtr reset</pre> <p>This issue only occurs in Cisco IOS Release 12.3(9a)BC when the <b>reset</b> command asks for confirmation to remove all the SAA related configuration. In Cisco IOS Release 12.2(15)BC2x , this issue is not present because the command does not ask for confirmation.</p> <p>Afterwards, entering any <b>show run</b> or configuration command causes the CLI interface to lockup for short period of time, and the following message is generated:</p> <pre>Unable to sync config-exited command to secondary</pre> <p>Workaround: Execute the following non service affecting command on the primary Performance Routing Engine (PRE):</p> <pre>hw-module sec-cpu reset</pre>
CSCsa95245	<p>Configuration information is lost when an OIR operation involves different types of line cards. This is the expected behavior of IOS.</p> <p>Workaround: The normal procedure is to manually save the interface configuration prior to removing the line card and restore it after the OIR is complete.</p>
CSCsb01435	<p>While trying to configure frequency stacking on C8/1, CMTS toggles configuration of US port so that the last US configured for the shared port is the only US enabled, and the 1st US configured for the same port is disabled.</p> <p>Workaround: When configuring FS on 2 cable LCs in the same slot (Cx/0 and Cx/1), even connectors need to be used on one line card and odd connectors on the other line card.</p> <p>Example:</p> <pre>Interface Cable 8/0/0   cable upstream 0 connector 0 shared   cable upstream 1 connector 0 shared Interface Cable 8/1/0   cable upstream 0 connector 1 shared   cable upstream 1 connector 1 shared</pre> <p>Depending on the current state of the configuration, it may be necessary to remove the upstream - connector mappings first:</p> <pre>no cable upstream &lt;n&gt; connector &lt;m&gt;</pre>
CSCsb02366	<p>QoS Prov for DOCSIS 2.0 cable modems very rightfully shows DOCSIS 1.0 or DOCSIS 1.1 because of the fact that the major difference between a modem running in DOCSIS 2.0 mode as opposed to DOCSIS 1.0/1.1 mode is the physical layer and not the QoS provisioning.</p> <p>In order to be consistent, we then should remove “DOC2.0” column under “QoS Provision” from “show cable modem mac summary” display.</p> <p>Additionally, we should also have “show cable modem phy summary” display to provide a quick summary of the cable modems in each phy mode on each interface.</p>

**Table 95** *Resolved Caveats for Cisco IOS Release 12.3(9a)BC7 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb17673	After performing multiple Performance Routing Engine (PRE) switchovers, several of the Protect and Working LCs may go into a non-functional state. Workaround: Reset the LC affected.
CSCsb21988	When using file mode of SAMIS, the XML data appears corrupted. There are no known workarounds.
CSCsb23279	The QID for the default queue on the Cable downstream interface is not correct. Depending on its value, the symptoms may vary. If the microcode for the Toaster should be reloaded, either manually via CLI or dynamically via a reset, this problem will persist. Workaround: Do not intentionally reload the microcode. Dynamic reloads cannot be avoided.
CSCsb28546	Voice RTP/UDP packets are not forwarded to CALEA DF (Server) after Line Card or Performance Routing Engine (PRE) switchover is performed. There are no known workarounds.
CSCsb30263	The E911 call stays connected after line card switchover, the E911 call was lowered to a regular active call from an ActiveHiPriCall. There are no known workarounds.
CSCsb30694	Repeated pxf unexpected reloads are observed with %PXF-2-FAULT: T1 Exception summary: CPU[t1r1c1] This occurs on a Cisco uBR10000 series router with a PRE1 platform running Cisco IOS Release 12.3(9a)BC3. There are no known workarounds.
CSCsb37635	CMTS unexpectedly reloads while the standby RP is loading. There are no known workarounds.

**Table 95** *Resolved Caveats for Cisco IOS Release 12.3(9a)BC7 (continued)*

<b>DDTS ID Number</b>	<b>Description</b>
CSCsb66664	<p>The bundle master interface does not come up, yet the slave interfaces does not have a problem.</p> <p>This issue occurs if the up converters are shutdown before making the interface. When this happens, the bundle master, then the up converters can not be enabled again as long as the interface is bundle master.</p> <p>Workaround: The bundle master configuration should be removed, and then the upconverter should be enabled. Then the interface should be made the bundle master while the up converters are enabled.</p>
CSCsb53506	<p>Service flows that specify a max latency parameter may get less bandwidth than expected.</p> <p>If the max latency is specified (non-zero) and the minimum reserved rate is not perfectly divisible by 8000, the remainder of the division is not accounted for and the policer associated with the service flow's queue will rate limit packets at a rate below the minimum reserved rate.</p> <p>This can have a significant impact to voice flows as 10% of packets will be rate limited and voice quality will be lower than expected.</p> <p>PRE2 engine, not PRE1 max latency, must be non-zero minimum reserved rate must not be perfectly divisible by 8000.</p> <p>For example, if the standard bit rate of 87,200 bps for G.711 is used, it is vulnerable to the bug since it is not perfectly divisible by 8000.</p> <p>Workaround: Specify the minimum reserved rate to be a multiple of 8000.</p>

## Open Caveats for Release 12.3(9a)BC6

This section documents possible unexpected behavior by Cisco IOS Release 12.3(9a)BC6 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(9a)BC6.

## Resolved Caveats for Release 12.3(9a)BC6

[Table 96](#) lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(9a)BC6.

**Table 96 Resolved Caveats for Cisco IOS Release 12.3(9a)BC6**

DDTS ID Number	Description
CSCef68324	<p>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.</p> <p>Cisco has made free software available to address this vulnerability for all affected customers.</p> <p>More details can be found in the security advisory that is posted at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050729-ipv6">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050729-ipv6</a></p>

## Open Caveats for Release 12.3(9a)BC5

This section documents possible unexpected behavior by Cisco IOS Release 12.3(9a)BC5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(9a)BC5.

## Resolved Caveats for Release 12.3(9a)BC5

Table 97 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(9a)BC5.

**Table 97 Resolved Caveats for Cisco IOS Release 12.3(9a)BC5**

DDTS ID Number	Description
CSCeb46784	<p>PHS rules generated by DSA or DSC are not synched to the Protect LC or the standby Performance Routing Engine (PRE).</p> <p>There are no known workarounds.</p>
CSCsb26840	<p>Packet drops on voice calls with PHS enabled when the maximum rate (MIR) for the voice stream is very close to the actual bandwidth used. You can notice this by picking up the phone and pressing a button. If you hear very short periods of silence interrupting the tone, that's it. Also, you can see if there are drops on the service flow by doing a <b>show int cx/y/z service-flow n counters verbose</b> for the service flow corresponding to downstream voice data.</p> <p>This issue occurs when PHS is enabled.</p> <p>Workaround: Turn off PHS or use cable modems which have large maximum rates (MIR) for voice data.</p>

## Open Caveats for Release 12.3(9a)BC4

This section documents possible unexpected behavior by Cisco IOS Release 12.3(9a)BC4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(9a)BC4.

## Resolved Caveats for Release 12.3(9a)BC4

Table 98 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(9a)BC4.

**Table 98** Resolved Caveats for Cisco IOS Release 12.3(9a)BC4

DDTS ID Number	Description
CSCeg77820	The standby Performance Routing Engine (PRE) does not boot to Hot Standby mode if there are more than 15 sub-interfaces configured on an interface. This problem is specific to PRE1. Workaround: Reduce the number of sub-interfaces.
CSCeh01845	Poor and irregular p performance results with 64 and 512-byte packet sizes on the Cisco IOS Release 12.3(9a)BC1 pre-fcs image. Workaround: Disable fragmentation by configuring “no cable upstream n fragmentation”.
CSCeh57367	Some CF functions do not correctly interpret flows where the traffic from one side has stopped because the other side has been placed on hold. The CMTS can change its behavior slightly to help them correctly replay these streams. There are no known workarounds.
CSCeh71709	The standby Performance Routing Engine (PRE) does not boot to HotStandby mode. There are no known workarounds.

**Table 98 Resolved Caveats for Cisco IOS Release 12.3(9a)BC4 (continued)**

DDTS ID Number	Description
CSCei00243	<p>In an MPLS-VPN environment, the LAN side IP address of customer premises equipment (CPE) router cannot be reached from a remote CMTS, and business customers on the LAN do not have connectivity.</p> <p>Workaround: Create a new loopback interface in a “TEST” vrf, routing traffic for the CPE “Lan” subnet to that new loopback interface, and then having another static route in the “TEST” vrf routing table that points back to the real location of the network.</p> <p>For example:</p> <p>In vrf “SP2” with CPE Router “WAN” IP 192.168.31.10 and “LAN” subnet is 99.99.99.0, instead of using the following static route on the Cisco uBR10000 series router:</p> <pre>ip route vrf ISP2 99.99.99.0 255.255.255.0 192.168.31.10</pre> <p>You would instead apply:</p> <pre>ip vrf TEST          ! The new "temporary" vrf  rd 9999:9999  !  interface Loopback9999 ! The new "temporary" loopback interface  ip vrf forwarding TEST  ip address 5.6.7.8 255.255.255.255  !  !  ip route vrf ISP2 99.99.99.0 255.255.255.0 Loopback9999 5.6.7.8 !  The IP  address of Loopback9999  !  ip route vrf TEST 99.99.99.0 255.255.255.0 Bundle 1.2 192.168.31.10  !  Replace Bundle 1.2 with the appropriate subinterface  !</pre> <p>The main drawback of this workaround is that it would be hard to scale for more than a few such network numbers.</p>
CSCsa69764	<p>SAMIS is enabled in Streaming Mode.</p> <p>If, for some reason, the Cisco uBR router was unable to send data to the server in the middle of streaming metering status is “write-error”; but when the destination server recovers, the cable metering status does not change and no more SAMIS information is exported to the server.</p> <p>There are no known workarounds.</p>
CSCsa71047	<p>When cable monitor is configured in a Cisco uBR10000 series router with FE0/0/0 as the outbound interface, no packets are captured on the monitoring station.</p> <p>This issue occurs because the Performance Routing Engine (PRE) is unable to reparent the packet before sending the packet out on the fastEthernet interface. The reason for not being able to reparent the particles is that there is no header pool for the cable hwidb in PRE.</p> <p>Workaround: Create a header pool for the cable interfaces as well.</p>

**Table 98 Resolved Caveats for Cisco IOS Release 12.3(9a)BC4 (continued)**

DDTS ID Number	Description
CSCsa71054	<p>When trying to change the fixed frequency to the frequency from non-shared spectrum-group with 40 spectrum-group used in Cisco uBR10000 series router running Cisco IOS Release 12.3(9a)BC1, the port was not assign the frequency from non-shared-spectrum-group.</p> <p>Before with the fixed image, cable upstream 2 frequency 32000000. After, with non-shared spectrum-group:</p> <pre>Router(config-if)#cab up 2 spec 1 Router(config-if)#^Z Router#sh cab spec 1 Group Frequency      Upstream      Weekly Scheduled      Power Shared No.   Band           Port          Availability          Level Spectrum       (Mhz)       From Time:    To Time: (dBmV) 1    Unassigned    Cable6/1/2      U2</pre> <p><b>Workaround One:</b> Avoid changing an upstream from a fixed frequency to the spectrum group, which has the same fixed frequency as its first one.</p> <p><b>Workaround Two:</b> Perform “cable up x shut” and then “no cable up x shut” if this issue occurs.</p>
CSCsa76002	<p>An unexpected upload occurs while adding deleting/adding a cable filter or ACL after doing show access list</p> <p>This issue occurs if show ACL list is performed. After some time, an ACL entry is deleted, possibly resulting in an unexpected upload.</p> <p><b>Workaround:</b> Do not perform show access list</p>
CSCsb00255	<p>The active Performance Routing Engine (PRE) suddenly stops seeing any of the line cards of the chassis. The ones that are seen, are seen via de SH CONTROLLERS in a bad state:</p> <pre>Show diag sees nothing but the PREs: Router#show diag sum Slot A: Primary PRE2-RP card Slot B: Secondary PRE2-RP card Show controllers sees the cards in bad stated (slot1 not even seen): Router#show controllers ..... ..... Interface GigabitEthernet4/0/0(idb 0x638B1EB4) Hardware is Half-height Gigabit Ethernet MAC Controller - Not initialized Interface GigabitEthernet7/0/0(idb 0x208370E4) Hardware is Gigabit Ethernet MAC Controller - Not initialized Interface GigabitEthernet8/0/0(idb 0x638BBC40) Hardware is Gigabit Ethernet MAC Controller - Not initialized</pre> <p><b>Workaround:</b> Reload any of the cards.</p>

**Table 98** *Resolved Caveats for Cisco IOS Release 12.3(9a)BC4 (continued)*

DDTS ID Number	Description
CSCsb02139	<p>Poor performance in cable modem best effort service flows in the downstream direction.</p> <p>This issue may occur when the Cable interface default queue has some amount of traffic. The more the traffic in default queue, the poorer the performance in BE queues. The default queue is usually used for downstream multicast traffic.</p> <p>There are no known workarounds.</p>
CSCsb05532	<p>The cable line card of the Cisco uBR10000 series router unexpectedly reloads and temporarily disconnects every user connected to that cable line card.</p> <p>This issue is exactly similar to the defect mentioned as DDTS # CSCeg14041, but the trigger which was causing the issue is different.</p> <p>Workaround: The unexpected reload was due to the stale flap pointer pointing to a freed chunk memory. It is recommended not to issue “clear cable flap-list all”.</p>

## Open Caveats for Release 12.3(9a)BC3

This section documents possible unexpected behavior by Cisco IOS Release 12.3(9a)BC3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(9a)BC3.

## Resolved Caveats for Release 12.3(9a)BC3

[Table 99](#) lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(9a)BC3.

**Table 99** *Resolved Caveats for Cisco IOS Release 12.3(9a)BC3*

DDTS ID Number	Description
CSCCef14781	<p>The Performance Routing Engine (PRE) reports the following error during a PRE switchover:</p> <pre>%UBR10K-3-QUEUEFULL: Unable to enqueue since the queue is full</pre> <p>There are no known workarounds.</p>
CSCCef77655	<p>When loading a PRE2 image onto a PRE1 card, the boot prompt changes to “invalid image for platform” and is never changed back; even after loading a good image.</p> <p>This issue occurs when loading a PRE2 image onto PRE1 card or vice versa.</p> <p>There are no known workarounds.</p>
CSCCef83385	<p>CPUHOG traceback messages appear on the cable line card (CLC) console during large-scale switchover.</p> <p>This issue occurs with ~39K CMs on a Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>

**Table 99 Resolved Caveats for Cisco IOS Release 12.3(9a)BC3 (continued)**

DDTS ID Number	Description
CSCef86161	<p>Traffic recovery after LC switchover may be inconsistent if BPI+ is configured and the default TEK lifetime/gracetime is changed.</p> <p>There are no known workarounds.</p>
CSCef89261	<p>LED on the Hot Standby Connection-to-Connection Protocol (HCCP) Protect interface keeps lighting up after switchback to the HCCP Working interface. This is cosmetic issue.</p> <p>This issue is cosmetic and occurs with N+1 redundancy with MC5x20 on Cisco IOS Release 12.2(15)BC2d.</p> <p>There are no known workarounds.</p>
CSCeg30130	<p>In CSCee32618, the user got a traceback following a “No current_if_info” message.</p> <p>There are no known workarounds.</p>
CSCeg44108	<p>A Cisco uBR 10000 series router may trigger an unexpected PXF processor reload.</p> <p>A large access-list must be applied on a Cable interface. The reload often occurs 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.</p> <p>The router will log the following messages:</p> <pre data-bbox="574 1045 1419 1150">%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</pre> <p>The PXF processor will resume operating, but may unexpectedly reload again in a cycle until the condition has been cleared.</p> <p>The unexpected reload occurs only when a split ACL is in use. Splits in ACLs can be observed with “show pxf cpu access-list security”.</p> <p>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.</p>
CSCeg55961	<p>The entPhysicalName needs to display the type of Performance Routing Engine (PRE) along with the interface name. So, basically it needs to specify whether the interface belongs to the active PRE or the standby PRE.</p> <p>Currently the output displays:</p> <pre data-bbox="574 1535 1062 1562">entPhysicalName.29 = FastEthernet0/0/0</pre> <p>It needs to be changed to:</p> <pre data-bbox="574 1608 1138 1635">entPhysicalName.29 = PRE_X:FastEthernet0/0/0</pre> <p>whereas “X” may be A or B. At any given time either “A” or “B” would be active or standby.</p> <p>There are no known workarounds.</p>
CSCeg58842	<p>This problem should only pop up if flow-aggregation of type prefix is enabled (the CLI is “ip flow-aggregation cache prefix”).</p> <p>There are no known workarounds.</p>

**Table 99 Resolved Caveats for Cisco IOS Release 12.3(9a)BC3 (continued)**

DDTS ID Number	Description
CSCeg71922	<p>One or more line 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).</p> <p>A crashinfo file is left on the line card with CPU Hog messages from the “CMTS Mac Timer” process, followed by a watchdog reset.</p> <p>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.</p> <p>The conditions for this issue are:</p> <ul style="list-style-type: none"> <li>• Line card must have been up for 49 days.</li> <li>• Service flows must have a non-zero activity timer.</li> <li>• PacketCable configurations are more vulnerable than pure data configurations because voice service flows typically use activity timers.</li> </ul> <p>This issue has been observed on uBR10k 520 line cards, but any cable configuration, including 7246, that uses service flow activity timers is vulnerable.</p> <p>Workarounds: The following are possible workarounds:</p> <ol style="list-style-type: none"> <li>1. Set the service flow activity timer to zero a few hours before the clock will rollover. Reenable the activity timer after the rollover.</li> <li>2. Check the uptime of the cards in the system, schedule a card reload prior to the rollover.</li> <li>3. If N+1 is configured: switch a card to the redundant card, reload the Working card and then revert. Repeat for all cards approaching the 49 day rollover point.</li> </ol> <p> <b>Note</b> The up time of a line card can be seen with the <b>show diag</b> command.</p>
CSCeg80463	<p>This issue is not reproducible.</p> <p>There are no known workarounds.</p>
CSCeh00967	<p>A Cisco BR10k series router running Cisco IOS Release 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 <b>show tech</b>.</p> <p>This issue occurs with cable spectrum-group configured on different cable interfaces, and if the total number of interface on the system needs exceeds 144</p> <p>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”.</p>

**Table 99 Resolved Caveats for Cisco IOS Release 12.3(9a)BC3 (continued)**

DDTS ID Number	Description
CSCeh37712	<p>This fix enables the LCHUNG process on the Cisco uBR10000 RP. This process will power cycle any hung cable line card. There is an exec command <b>auto-clc-hang-reset onloff</b> which can disable or enable the polling. The default will be enable.</p> <p>There are no known workarounds.</p>
CSCeh42526	<p>The LCHUNG process on a Cisco uBR10000 series router does 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.</p> <p>There are no known workarounds.</p>
CSCeh43502	<p>The router unexpectedly reloads while modifying/applying mcast access list. This issue occurs with failure in creation of multicast service flow first, followed by modifying/applying of mcast access list</p> <p>There are no known workarounds.</p>
CSCin87617	<p>CMTS unexpectedly reloads while the modem is trying to get authenticated with the Authentication, Authorization, and Accounting (AAA) server.</p> <p>Cable privacy authenticate-modem CLI was configured and the unexpected reload occurs only if debug radius is enabled in CMTS. This is easily reproducible with MC28C as well as MC520S testbeds.</p> <p>This issue occurs under the following and is verified to exist in Cisco IOS Releases 12.2(15)BC2e and 12.3(9a)BC1:</p> <pre>debug radius cable privacy authenticate-modem</pre> <p>Workaround: Do NOT attempt to debug radius while using “cable privacy authenticate-modem”.</p>
CSCsa47427	<p>With dynamic secret enabled, if ALL conditions described below are true, modems may get stuck in init(o) state and fail to register.</p> <p>The conditions are:</p> <ol style="list-style-type: none"> <li>1. Each modem gets its own config file (for e.g. as when BACC is used for provisioning).</li> <li>2. The CM config files are large (greater an 1024 bytes in size).</li> <li>3. Large number are trying to connect to the CMTS.</li> <li>4. The RP CPU is high (close to 100%).</li> </ol> <p>Workaround: The only workaround is to reduce the number of modems trying to connect to the CMTS at the same time. This includes increasing insertion interval and ranging backoffs, shutting down interfaces or upstreams.</p>
CSCsa50929	<p>The fix for CSCsa48673 will cause US Load Balancing to not decrement the Pending count.</p> <p>There are no known workarounds.</p>

**Table 99 Resolved Caveats for Cisco IOS Release 12.3(9a)BC3 (continued)**

DDTS ID Number	Description
CSCsa54614	<p>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. But 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.</p>
CSCsa59110	<p>ACLs with 8 or more entries may not work according to the configured rules. This issue occurs with ACLs that have 8 or more entries. There are no known workarounds.</p>
CSCsa59295	<p>On a Cisco uBR10000 series platform, the Performance Routing Engine (PRE) unexpectedly reloads. The unexpected reloads reported may contain: System returned to ROM by bus error at PC 0x&lt;varies&gt;, address 0xB0D0B5D at (time)...</p> <p>These issues may occur under stress situations with large numbers of unstable cable modems (modems do not stay online and cause their arp entries to be deleted), and intensive SNMP polling of the entire cable modem database, the Cisco uBR10000 series router may experience PRE failovers. In particular, querying the atEntry table will cause the problem.</p> <p>The fault has been observed in Cisco IOS Releases 12.2(15)BC2d, BC2e, BC2f, and 12.3(9a)BC, 12.3(9a)BC2. A specific testbed was able to reproduce this crash about once every 12-36 hours.</p> <p>Workaround: Disable intensive SNMP polling. Improve modem stability. Utilize redundant PREs, and the system will remain operational. The redundant PRE will take over successfully, the failed PRE will recover, and be available before the redundant PRE fails again.</p>
CSCsa63951	<p>Poor performance may be observed such as Voice over IP (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.</p> <p>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.</p> <p>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 <math>500 * 64 / 6.25 = 5120</math>.</p>

Table 99 Resolved Caveats for Cisco IOS Release 12.3(9a)BC3 (continued)

DDTS ID Number	Description
CSCsa69875	<p>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 &lt;modem ip addr&gt;” will be empty.</p> <p>This issue occurs when the cable interface command <b>cable arp filter reply-accept &lt;packets&gt; &lt;time window&gt;</b> is present and virus activity is high on the CMTS.</p> <p>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:</p> <pre>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</pre> <p>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.</p> <p>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:</p> <p><a href="http://homesupport.cisco.com/en-us/support/linksys">http://homesupport.cisco.com/en-us/support/linksys</a></p> <p>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.</p>
CSCsa72839	<p>Crash of type “PXF DMA Error - Small Packet Handle Creating a Large Descriptor, Restarting PXF”.</p> <p>This issue occurs with mutlicast echo enabled and output ACL configured on a cable interface. Multicast packet upstream goes through multicast echo and gets dropped because of output ACL. Also the packet size is large (roughly greater than 512 bytes).</p> <p>Workaround: Turn off multicast echo or remove output ACL from the affected cable interface. To turn off multicast echo use the interface command <b>no cable ip-multicast-echo</b>.</p>

**Table 99 Resolved Caveats for Cisco IOS Release 12.3(9a)BC3 (continued)**

DDTS ID Number	Description
CSCsa76715	<p>Frequent SNMP queries of the Cisco uBR10000 arp table by ipNetToMediaTable or atEntry will result in high CPU usage by the SNMP ENGINE process, upwards to 80%.</p> <p>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.</p> <p>This issue occurs on 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.</p> <p>Although SNMP will usually appear to use high CPU, this problem was made worse on the Cisco IOS Release 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 Cisco IOS Release 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.</p> <p>Workaround: The following are possible workarounds:</p> <ol style="list-style-type: none"> <li>1. If an extreme problem, turn off querying. If snmp servers can't be isolated, setup an ACL on port 161.</li> <li>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.</li> <li>3. Exclude the ipNetToMediaTable from querying. The following config will achieve this: <pre>snmp-server view noarp ipNetToMediaEntry excluded snmp-server view noarp iso include snmp-server community public view noarp ro.</pre> <p>The impact of 3 is that there will be no results returned to the tool.</p> </li> <li>4. Exclude 3 of the 4 subtables of ipNetToMediaTable. This will cut the querytime by 75%: <pre>ipNetToMediaTable is comprised of 4 tables: ipNetToMediaIfIndex      aka ipNetToMediaEntry.1 ipNetToMediaPhysAddress aka ipNetToMediaEntry.2 ipNetToMediaNetAddress  aka ipNetToMediaEntry.3 ipNetToMediaType        aka ipNetToMediaEntry.4</pre> </li> </ol>

Table 99 Resolved Caveats for Cisco IOS Release 12.3(9a)BC3 (continued)

DDTS ID Number	Description
	<p>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.</p> <p>Example:</p> <pre>ipNetToMediaPhysAddress.2.10.11.1.15 = 00 05 00 e5 35 d4</pre> <p>A sample configuration that includes just ipNetToMediaPhysAddress is:</p> <pre>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</pre> <p>Such a config 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.</p> <p>For reference, here is the sample output showing how one arp entry creates four results records from the ipNetToMediaTable query:</p> <pre>ipNetToMediaIfIndex.7.50.3.81.1 = 7 ipNetToMediaPhysAddress.7.50.3.81.1 = 00 05 00 e5 36 10 ipNetToMediaNetAddress.7.50.3.81.1 = 50.3.81.1 ipNetToMediaType.7.50.3.81.1 = static(4)</pre> <p>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%.</p>
CSCef93215	<p>A router that is configured for OSPF reloads unexpectedly and references the “ospf_build_one_paced_update” process.</p> <p>This issue occurs 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 symptom may occur at any time without any specific changes or configuration and is not specifically related to any type of LSA.</p> <p>There are no known workarounds.</p>
CSCeh20178	<p>Stabilize periodic station maintenance scheduling. This fix is necessary for cable domains with more than 2000 modems on a single downstream.</p> <p>There are no known workarounds.</p>
CSCsa53912	<p>You cannot log on when a TACACS+ server is used for authentication. You get a message that authentication fails and you are asked again to enter your user name.</p> <p>This issue occurs when you make a Telnet connection to a router that is configured for TACACS+ after you have entered your user name and your TACACS password.</p> <p>Workaround: Configure the TACACS+ single connection option by entering the <b>tacacs-server host host-name single-connection</b> command.</p>

## Open Caveats for Release 12.3(9a)BC2

This section documents possible unexpected behavior by Cisco IOS Release 12.3(9a)BC2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(9a)BC2.

## Resolved Caveats for Release 12.3(9a)BC2

Table 100 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(9a)BC2.

**Table 100** Resolved Caveats for Cisco IOS Release 12.3(9a)BC2

DDTS ID Number	Description
CSCeh20178	Stabilizes periodic station maintenance scheduling. This fix is necessary for cable domains with more than 2000 modems on a single downstream.  There are no known workarounds.
CSCsa63951	Poor performance may be observed, such as Voice over IP (VoIP) latency, dropped packets, uncorr FEC errors under the <b>sh cab hop</b> 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 issues 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”. For 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 $500 * 64 / 6.25 = 5120$ .

## Open Caveats for Release 12.3(9a)BC1

This section documents possible unexpected behavior by Cisco IOS Release 12.3(9a)BC1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.3(9a)BC1.

## Resolved Caveats for Release 12.3(9a)BC1

Table 101 lists only severity 1 and 2 caveats and select severity 3 caveats for the Cisco IOS Release 12.3(9a)BC1.

**Table 101** Resolved Caveats for Cisco IOS Release 12.3(9a)BC1

DDTS ID Number	Description
CSCef35392	<p>All Cable Modems on unspecified DS of a Cisco uBR10-MC5X20U card become offline after a Hot Standby Connection-to-Connection Protocol (HCCP) switchover and stay in the “offline” state.</p> <p>The <b>show controller cable</b> <i>x/y/z</i> command shows “No MAP buffer” incrementing and the “UCD Count” for each upstream stuck.</p> <p>This issue occurs when conducting HCCP N+1 redundancy with Cisco uBR10-MC5X20U on Cisco IOS Release 12.2(15)BC2b.</p> <p>Workaround: Enter the <b>hw-module subslot</b> <i>x/y</i> <b>reset</b> command to reset the LC.</p>
CSCef40864	<p>It is possible that when a cable bundle slave interface is shut/no shut, it cannot repopulate the cable bundle forwarding table with some IGMP static group defined on master interface.</p> <p>There are no known workarounds.</p>
CSCef54096	<p>A Cisco uBR10000 series router unexpectedly reloads due to IP INPUT process.</p> <p>There are no known workarounds.</p>
CSCef64537	<p>The HCCP <b>unlock</b> command causes a CMTS to unexpectedly reload intermittently.</p> <p>This issue occurs when using the HCCP <b>unlock</b> command.</p> <p>There are no known workarounds.</p>
CSCef70739	<p>A “MAXMEMORY USED Reached maximum amount of memory allocated for stile” error is displayed at the console and the “Active links” for the <b>show ip nbar resources</b> command will show 4 GB plus.</p> <p>When the NBAR feature is activated, that is, when <b>match protocol</b> <i>protocol-name</i> is included in a policy map, or <b>ip nbar protocol-discovery</b> is applied on an interface, the “MAXMEMORY USED Reached maximum amount of memory allocated for stile” error may appear on the console.</p> <p>Workaround: Perform <b>no ip nbar resources</b> to reset active links back to zero.</p>
CSCef75363	<p>After a N+1 switchover, the ARP entry for customer premises equipment (CPE) devices is 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.</p> <p>Workaround. CPE traffic will recover without any user intervention.</p>
CSCef75566	<p>During LC switchover, the slave interface does not sync over any IGMP Static Group.</p> <p>Workaround: Reconfigure the IGMP static group on master interface.</p>

**Table 101 Resolved Caveats for Cisco IOS Release 12.3(9a)BC1 (continued)**

DDTS ID Number	Description
CSCef79820	<p>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.</p> <p>This issue occurs in the docsis-mode is tdma-atdma (mix) mode in Cisco IOS Release 12.2(15)BC2a and later releases.</p> <p>Workaround: Use “cable upstream x shutdown” and “no cable upstream x shutdown”.</p>
CSCef87118	<p>In Cisco IOS Release 12.2(15)BC2c, the DHCPD Receive process may hold memory when DMIC is used.</p> <p>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.</p> <p>There are no known workarounds.</p>
CSCef94945	<p>When the router is coming out of startup and the initial table_id write to toaster memory is performed the write would fail, the toaster was not ready for the write to toaster memory at this time.</p> <p>Code has been added to perform the toaster write when the toaster is available after startup.</p> <p>There are no known workarounds.</p>
CSCeg05210	<p>If the CMTS cable arp request filter is configured to filter all arp requests, it appears to not filter at all. In reality, all arp requests are being filtered, but not statistically accounted for.</p> <p>Example config:</p> <pre>interface Cable8/0/0 ...   cable arp filter request-send 0 2</pre> <p>Example output:</p> <pre>show cable arp-filter Cable8/0/0 ARP Filter statistics for Cable8/0/0:   Replies Rcvd: 22 total. 0 unfiltered, 0 filtered   Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered   Requests Forwarded: 2000 total. 0 unfiltered, 0 filtered</pre> <p>Note that Requests Forwarded “filtered” count is 0.</p> <p>Note that this is an unusual configuration because if the arp request filter is set to filter all packets, modems will not come online. So this configuration is only used for debug purposes.</p> <p>All versions of CMTS software that support the cable arp filter feature on Cisco IOS Releases 12.2(15)BC2 and 12.3(9)BCa. To be fixed in Cisco IOS Release 12.3(9)BCb.</p> <p>There are no known workarounds.</p>
CSCeg05586	<p>Voice calls fail on a Cisco uBR10000 series router running Cisco IOS Release 12.3(8.4)BC. Specifically, the downstream dynamic service flow is dropping packets.</p> <p>There are no known workarounds.</p>

**Table 101 Resolved Caveats for Cisco IOS Release 12.3(9a)BC1 (continued)**

DDTS ID Number	Description
CSCeg07988	<p>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.</p> <p>If SNMP set is done, it will show the update Val. It will also update the modulation profile in the CMTS CLI, but the modems will not apply it to the modems.</p> <p>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.</p> <p>This issue was observed on Cisco IOS Release 12.2(15)BC2b on a Cisco uBR10000 series router with a PRE1 and a MC520 card.</p> <p>Workaround: Use the CLI to change the modulation profiles.</p>
CSCeg12481	<p>DHCP Proxy feature configured on the Cable Modem, is not supported by CMTS.</p> <p>The CMTS is dropping the DHCPOFFER from the DHCP server if the ip address assigned to the customer premises equipment (CPE) does not belong to any directly connected interface.</p> <p>This problem is being triggered by CSCee84392.</p> <p>This message is the one that could be seen if DHCP debug is enabled:</p> <pre data-bbox="573 968 1481 1052">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</pre> <p>There are no known workarounds.</p>
CSCeg14041	<p>A Cisco uBR10000 series router with PRE1-RP processor running Cisco IOS Release 12.2(15)BC2d reloads unexpectedly with a bus error after an interface flapping. The sequence and error message would be seen as follows:</p> <pre data-bbox="573 1199 1481 1335">%UBR10000-6-CMOVED: Cable modem &lt;MAC_address&gt; 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</pre> <p>There are no known workarounds.</p>
CSCeg17018	<p>Some single bit ECC errors will unexpectedly reload the 520S-D line card, even though the GT64120 controller can handle single bit ECC errors.</p> <p>There are no known workarounds.</p>
CSCeg23455	<p>The PXF queue allocation fails due to insufficient queue resources, even though there are only small number of queues on the interface.</p> <p>Further investigation found that the problem was caused by stale secondary (dynamic) service flows on the RP.</p> <p>It is unclear what conditions causes this problem, but it is likely to have been induced by a Performance Routing Engine (PRE) switchover.</p> <p>Workaround: Clear the cable modems to which the stale service flow belongs.</p>
CSCeg28052	<p>When the MTAs are on the bundle slave interface, there is no call content for CALEA calls for the Cisco uBR10000 series router.</p> <p>Workaround: Configure the MTAs on bundle master or non-bundle interface.</p>

**Table 101 Resolved Caveats for Cisco IOS Release 12.3(9a)BC1 (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCeg30535	<p>CM config files with Min Reserved Traffic Rate set to zero was being handled wrong in the PRE2.</p> <p>This value must be set to a non-zero value else the SF gets no bandwidth at all, resulting in all packets dropped on the DS.</p> <p>There are no known workarounds.</p>
CSCeg36445	<p>A Cisco universal broadband router reloads unexpectedly as a result of its memory getting corrupted. This causes a switchover to the standby Performance Routing Engine (PRE).</p> <p>There are no known workarounds.</p>
CSCeg41331	<p>PRE2 punt ISR to handle diverted packets from the pxf engine to the RP processor is not implemented as an inline “C” function. The PRE1 function is implemented as an inline function. That leads to slightly slower performance on PRE2 compared to PRE1.</p> <p>There are no known workarounds.</p>
CSCeg42335	<p>A Cisco uBR10012(Pre1) Broadband Router may experience a packet latency/loss issue on cable interfaces when <b>cable source-verify [dhcp]</b> is configured.</p> <p>This issue occurs on a Cisco uBR10012(PRE1) Broadband Router that runs Cisco IOS Release 12.2(15)BC02 when the cable interfaces have <b>cable source-verify [dhcp]</b> configured. The symptom may occur also in other releases.</p> <p>Workaround: Turn off source verify. Reload the box, shutdown all the cable interfaces (or all the cable bundle master interfaces), and then bring them up one by one. Micro reload pxf switchover.</p>
CSCeg56960	<p>The following happens on the line card when a Performance Routing Engine (PRE) switchover happens:</p> <pre>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</pre> <p>This issue occurs if all ipc traffic is not properly cleared.</p> <p>There are no known workarounds.</p>
CSCin71099	<p>Switchover from MC520u to MC520s occurs, but switchover from MC520s to MC520u is NOT support in this release.</p> <p>Only MC520s to MC520s and MC520u to MC520u is supported.</p> <p>There are no known workarounds.</p>
CSCin80987	<p>In a HA enabled CMTS, if a <b>clear cable modem</b> CLI is invoked and the CMTS any time later performs a Performance Routing Engine (PRE) switchover and QoS profile reference counts on the standby PRE will be completely wrong.</p> <p>This causes QoS profile deletion/addition behavior to be totally wrong after the switchover for all times to come.</p> <p>There are no known workarounds.</p>

**Table 101** *Resolved Caveats for Cisco IOS Release 12.3(9a)BC1 (continued)*

DDTS ID Number	Description
CSCin84603	<p>Executing the <b>no debug all</b> command or the <b>undebug all</b> can result in the following error message, along with a traceback:</p> <pre>%SCHED-7-WATCH: Attempt to enqueue uninitialized watched queue (address 0).</pre> <p>This problem occurs only when an SRP/OC-12 line card is installed in the CMTS. There are no known workarounds.</p>
CSCsa41720	<p>A Cisco uBR10000 CMTS router with PRE1 may unexpectedly reloads while unconfiguring routing protocols or changing or removing the ip address on interface. There are no known workarounds.</p>
CSCsa44591	<p>Tacacs TCP session between router and ACS hangs with the single connection option. This issue occurs on a Cisco uBR router running Cisco IOS Release 12.3(9a)BC. Workaround: Remove the “single-connection” option with the Tacacs+ config. When this issue occurs, turn off and turn on the “single connect” option.</p>

## Open Caveats for Release 12.3(9a)BC

Table 102 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(9a)BC.

**Table 102** *Open Caveats for Cisco IOS Release 12.3(9a)BC*

DDTS ID Number	Description
CSCeb25866	<p>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.</p>
CSCec04915	<p>Intermittent ping failure is seen on the GE. There are no known workarounds.</p>

**Table 102**      **Open Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCec35079	<p>Under certain load conditions, modems may be stuck in init(rc) or other pre-registration states.</p> <p>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.</p> <p>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.</p> <p>With some modem types, it is also observed that affected modems start to request bandwidth with SID 0.</p> <p>Note that this condition <i>_only_</i> occurs if, with above mentioned conditions, the upstream utilization is <i>_constantly_</i> at its capacity, i.e., well above 90%.</p> <p>The upstream utilization can be checked with the <b>show interface interface mac-scheduler n</b> command where <i>interface</i> is the cable interface and <i>n</i> is the upstream channel.</p> <p>The output of this command will include the line Avg upstream channel utilization: xx%.</p> <p>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).</p> <p>There are no known workarounds.</p>
CSCed07010	<p>If before a Performance Routing Engine (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.</p> <p>Workaround: Do a hw-module reset of the Protect interface.</p>
CSCed89210	<p>When there is heavy traffic on the backhaul interface and the Cisco uBR10000 series 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'</p> <p>Workaround: Ensure that the traffic coming to the router is not very heavy immediately after bootup.</p>
CSCee00895	<p>In a Cisco uBR10000 series router, packets switched by PXF are counted as process switched packets for the backhaul interfaces. While this provides accurate information for SNMP and the <b>show interface</b> command it may not accurately reflect the performance of the router as viewed via the <b>show interface switching</b> command. The IP protocol counters displayed by that variant of the show command adds the number of PXF switched packets to the number of process switched packets and may give the impression that packets are being switched by the routing processor instead of the PXF hardware.</p> <p>Workaround: For receive packets, the <b>show pxf cpu statistics diversion</b> command can be used to see how many packets were diverted to the RP per line card. Subtracting that number from the interface's input counter will show if the majority of packets are being PXF switched for a given interval.</p> <p>No such workaround exists for output packets.</p>

**Table 102** Open Caveats for Cisco IOS Release 12.3(9a)BC (continued)

DDTS ID Number	Description
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 cable modem termination system (CMTS) reports a traceback error during a Performance Routing Engine (PRE) switchover. There are no known workarounds.
CSCee41060	pstream Timing offsets not synced over to Protect line card 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). Alternative workaround: Configure a high safety value in the dynamic map advance CLI command.
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.
CSCee94943	SID not provided when running command “sh hard pxf cable source-verify”. This issue was seen internally while testing modem reset the modem needs to be assign to a subinterface via DHCP. There are no known workarounds.
CSCef01314	The RF Switch takes 2~5 seconds for an SNMP-response. When doing “sh hccp channel switch”, it is talking to each module in the RF Switch that comprises the bitmap and taking an extremely long time to timeout, instead of just talking to the RF Switch to verify connectivity. The snmp RW string is “private” by default, but can be changed in the RF Switch. If the RW “private” string is changed or deleted in the router, it could have adverse affects on communications between the devices as well. Workaround: Make a hard-break possible to stop the command from executing. Then do “sh hccp g m channel” to look at each individual member of a group individually.
CSCef14781	The Performance Routing Engine (PRE) reports the error below during a PRE switchover: %UBR10K-3-QUEUEFULL: Unable to enqueue since the queue is full There are no known workarounds.
CSCef28979	If the host IP address is changed after the CM is online, the host IP address is not synched to the standby Performance Routing Engine (PRE) or Protect LC. This would cause delays in traffic recovery after a PRE or LC switchover. There are no known workarounds.

**Table 102** Open Caveats for Cisco IOS Release 12.3(9a)BC (continued)

DDTS ID Number	Description
CSCef30185	<p>The following “Unknown type” error messages may appearing at the CMTS console after the following actions do N+1 switchover (or) shut/noshut on cable interface:</p> <pre>Jul 29 09:06:44.899: Unknown type 16843263 Jul 29 09:06:44.899: Unknown type -16709634</pre> <p>There are no known workarounds.</p>
CSCef31547	<p>Cisco modems and possibly modems using BCM3300 chip could have timing problems and ranging issues on the MC520s card when running in sparse mode.</p> <p>There are no known workarounds.</p>
CSCef36045	<p>Bundle entries on the Cisco uBR10000 series router do not get aged.</p> <p>There are no known workarounds.</p>
CSCef48680	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.2(15)BC2b experiences multiple Performance Routing Engine (PRE) reloads and switchovers due to keepalive timeout triggered because of IPC cache exhaustion.</p> <p>The following messages are seen in the logs before the reload:</p> <pre>%IPC-3-NOBUFF: The main IPC message header cache is empty -Traceback= 6062E120 6062EA28 6062E990 60622CE4 606243A4 60E1464C 6065F90C 6068DB48 60034980 %C10K-2-RPRTIMEOUT_CRASH: Performing crashdump and switchover due to keepalive timeout %Software-forced reload</pre> <p>The Primary PRE performs a switchover to the Secondary PRE automatically.</p> <p>There are no known workarounds.</p>
CSCef49675	<p>CMTS customer premises equipment (CPE) Host entry will be deleted if after the arp time-out the arp response is not received from CPE, and arp refresh fails, in which case the arp entry is also deleted.</p> <p>However there are certain cases which is not consistent with the above behavior, and where the arp entry is deleted but the host entry is not deleted. These cases are as follows:</p> <ol style="list-style-type: none"> <li>1. If line protocol on the master interface flaps.</li> <li>2. If the interface ip address is removed and added again.</li> <li>3. If Sub-interface is deleted and re-added.</li> <li>4. If Dynamic Arp entry is removed by using the config command <b>no arp</b>.</li> </ol>
CSCef52564	<p>It is possible when using the Cisco uBR10000 series router with RF Switches and HA configured that DOCSIS sync message restoration does not resume within the specification requirement of 200 msec.</p> <p>There are no known workarounds.</p>

**Table 102**      **Open Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCef54302	<p>A Cisco uBR10000 series router with redundant Performance Routing Engines (PREs) might run into a situation where dir on sec-disk0: and sec-bootflash: does not yield relevant output.</p> <p>The error message “Error Sending Request” is generated when a “dir sec-disk0:” and “dir sec-bootflash” is performed.</p> <p>This issue may occur due to heavy load (huge number of cable modems on the CMTS).</p> <p>There are no known workarounds.</p>
CSCef55523	<p>A Cisco uBR10012 CMTS running Cisco IOS Release 12.2(15)BC2d may not pass traffic on Gigabit Ethernet interfaces after a reload/upgrade.</p> <p>Workaround: Reload the CMTS.</p>
CSCef60827	<p>A Cisco uBR10012 running Cisco IOS Release 12.2(15)BC2d could hang if OSPF hello packets are sent out the cable interface. Note that OSPF adjacencies are not supported on cable interfaces.</p> <p>Workaround: Configure all cable interfaces as “passive-interface”.</p>
CSCef61006	<p>After a Performance Routing Engine (PRE) switchover, standby PRE reloads unexpectedly when configuration mode is entered and exited on the active PRE.</p> <p>Workaround: Wait until the standby PRE is in Hot Standby before entering the configuration mode on the active PRE.</p>
CSCef64537	<p>The HCCP <b>unlock</b> command causes a CMTS to reload intermittently.</p> <p>This issue occurs with the HCCP <b>unlock</b> command.</p> <p>There are no known workarounds.</p>
CSCef66578	<p>The output of the <b>show cable modem connectivity</b> command displays an extremely large value.</p> <p>This issue occurs in Cisco IOS Release 12.2(15)BC2b and 12.2(15)BC2c.</p> <p>There are no known workarounds.</p>
CSCef67230	<p>A 520 card can lose its IPC connectivity to its Performance Routing Engine (PRE) causing the PRE to fail keepalive to the card and subsequently resetting the cable line card (CLC) causing all modems on the 520 card to go offline.</p> <p>There are no known workarounds.</p>
CSCef75363	<p>After a N+1 switchover, the ARP entry for customer premises equipment (CPE) devices is 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.</p> <p>Workaround. CPE traffic will recover without any user intervention.</p>
CSCef78175	<p>For CM-created qos profiles for DOCSIS 1.0 modems, on a Cisco uBR10000 series router after a “clear cable modem all delete”, if an LC switchover is initiated, the qos profile internal reference count used in addition/deletion of qos profiles will get messed up - the switchover leads to incorrect values for reference count on the Performance Routing Engine (PRE) and the switched over LC.</p> <p>There are no known workarounds.</p>

**Table 102 Open Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCef79820	<p>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.</p> <p>This issue occurs in the docsis-mode is tdma-atdma (mix) mode in Cisco IOS Release 12.2(15)BC2a and later releases.</p> <p>Workaround: Use “cable upstream x shutdown” and “no cable upstream x shutdown”.</p>
CSCef86372	<p>A Cisco uBR10000 series router may reload unexpectedly.</p> <p>The following unusual entry was observed in logs just before the reload:            %C10K-5-REDCHANGE: EHSA Register changed Prev.            This issue could be related to redundancy configured with no standby Performance Routing Engine (PRE).            There are no known workarounds.</p>
CSCef87118	<p>In Cisco IOS Release 12.2(15)BC2c, the DHCPD Receive process may hold memory when DMIC is used.</p> <p>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.</p> <p>There are no known workarounds.</p>
CSCef87302	<p>Add Option 82 to DHCPRENEW &amp; DHCPRELEASE messages that pass through the CMTS which is a relay agent. The feature has to be implemented for both modem and customer premises equipment (CPE) DHCP traffic.</p> <p>There are no known workarounds.</p>
CSCef92997	<p>A Cisco uBR router unexpectedly reloads with software forced reload after:</p> <pre>Aug 10 13:58:27.692: %SYS-2-FREEFREE: Attempted to free unassigned memory at 638BB58C, alloc 60945BC4, dealloc 60946A9C Aug 10 13:58:27.696: %SYS-6-BLKINFO: Attempt to free a block that is in use blk 638BB564, words 118, alloc 60945BC4, Free, dealloc 60946A9C, rfcnt 0 Aug 10 13:58:27.728: %SYS-2-MALLOCFAIL: Memory allocation of 328 bytes failed from 0x60914A58, alignment 0 Pool: Processor Free: 408351600 Cause: Mempool corrupt Alternate Pool: None Free: 0 Cause: No Alternate pool</pre> <p>There are no known workarounds.</p>
CSCef93561	<p>With a large number of modems, the system may report IPC errors during a N+1 switch over.</p> <p>There are no known workarounds.</p>
CSCef93714	<p>Illegal cloned modems still receive cable service even in reject (pk) state.</p> <p>There are no known workarounds.</p>
CSCin79597	<p>In a fully loaded CMTS, after doing a OIR on the Working cable line card (CLC) some of the modems, may get reset on some Downstreams.</p> <p>There are no known workarounds.</p>

## Resolved Caveats for Release 12.3(9a)BC

Table 103 lists only severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.3(9a)BC.

**Table 103** Resolved Caveats for Cisco IOS Release 12.3(9a)BC

DDTS ID Number	Description
CSCea08812	<p>If a client leaves the multicast group the CMTS will continue to forward multicast traffic on that interface.</p> <p>This issue is observe when running multicast over bundle interfaces.</p> <p>This only causes a performance problem because unnecessary traffic is consuming the available bandwidth.</p> <p>There are no known workarounds.</p>
CSCea68692	<p>If the <b>crypto key generate rsa</b> command is configured on a Cisco uBR10000 CMTS with dual Performance Routing Engines (PREs), the command fails to synchronize to the secondary PRE. This issue is a duplicate of CSCdw08393.</p> <p>This issue occurs with a <b>crypto key generate rsa</b> command with dual PRE on the Cisco uBR10000 series router.</p> <p>Workaround: Reset the secondary PRE.</p>
CSCea82892	<p>The <b>clear cable flap-list all save-counters</b> does not save the counters.</p> <p>This issue occurs only on the Cisco uBR10000 series router.</p> <p>There are no known workarounds.</p>
CSCeb71709	<p>The Cisco uBR router can only support 1 root certificate, which means that 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.</p> <p>There are no known workarounds.</p>
CSCec07639	<p>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.</p> <p>The issue 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.</p> <p>Workaround: Disable DMIC.</p> <p>Alternative Workaround: Edit the config file so that it is less than 4096 bytes in length.</p>
CSCec27338	<p>Network Based Access Recognition (NBAR) is used to classify packet streams.</p> <p>When packet streams contain packets that are fragmented it is 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.</p> <p>There are no known workarounds.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCec48483	<p>Upon reloading both the active and standby Performance Routing Engines (PREs), after the system comes up, the Protect line card comes up correctly, but the Working line card is in the down state.</p> <p>This is a rare condition that is not easily reproducible.</p> <p>Workaround: Perform a hw_module reset at the Working line card.</p>
CSCec68998	<p>Per interface diversion counts are not available in a Cisco uBR10000 series router. Further, the number of these packets being enqueued to the process level is also not available through any show command.</p> <p>There are no known workarounds.</p>
CSCec83821	<p>The CMTS may fail to register modems correctly when the <b>TFTP-Enforce</b> command is enabled. The CMTS may display the message below:</p> <pre data-bbox="613 743 1528 821">%UBR10000-4-REGISTRATION_BEFORE_TFTP_MARK: Registration request unexpected: Cable Modem did not attempt TFTP. Modem marked with #. CM Mac Addr &lt;xxxx.xxxx.xxxx&gt;</pre> <p>There are no known workarounds.</p>
CSCed21438	<p>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 ACLs that are installed in the CM DOCSIS config file.</p> <p>This issue occurs when running <b>cable dhcp-giaddr policy</b> 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.</p> <p>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.</p> <p>There are no known workarounds.</p>
CSCed26897	<p>Every frequency hop leads to an upstream re-init which in current SW can case a 300ms delay in servicing UGS. The issue 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</p> <p>There are no known workarounds.</p>
CSCed29019	<p>When a Cisco 10K Gigabit Ethernet card is directly connected to a cat4k Gigabit Ethernet card, link negotiation between the two fails. C10K says that link is UP, cat4k says link is DOWN.</p> <p>A 15 msec delay is needed to allow autonegotiation between these 2 interfaces.</p> <p>There are no known workarounds.</p>
CSCed46270	<p>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 Hot Standby Connection-to-Connection Protocol (HCCP) switchover. Traffic to and from modems on the subinterface affected will be impacted.</p> <p>Workaround: Perform another HCCP (LC) switchover to clear the problem.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCed49070	<p>The standby PRE could reload during boot up due to inconsistencies. No action is required by the user.</p> <p>There are no known workarounds.</p>
CSCed53225	<p>Due to excessive memory fragmentation, call to malloc fails even though available free memory may be greater than the requested size.</p> <p>There are no known workarounds.</p>
CSCed55021	<p>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.</p> <p>Workaround: Reduce the number of secondary IP addresses configured on a cable interface.</p> <p>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.</p>
CSCed65223	<p>The ifHCOctets counters are impossibly high for Gigabit Ethernet interfaces. This issue occurs on Cisco uBR10000 series routers running Cisco IOS Release 12.2(15)BC1. However, the ifHCInOctets counters seem to work correctly.</p> <p>There are no known workarounds.</p>
CSCed65409	<p>Bogus ARP entries are created when multiple DHCP servers reply with their offers.</p> <p>This can significantly increase memory consumption when many CMs are trying to register. It also causes the router to perform unnecessary arp entry addition.</p> <p>This is a result of bad sync.</p> <p>There are no known workarounds.</p>
CSCed68829	<p>Some modems might not be queried from SNMP cdxCmCpeTable and line card CLI "show cable device access-group".</p> <p>Workaround: shut/no shut cable interface.</p>
CSCed68879	<p>Running Cisco IOS Release 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</p> <p>Workaround: For MC16S cards use the CNR value from '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.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCed70180	<p>Certain modems, when configured in routing mode, might not be able to pass IP traffic when DMIC is enabled on the CMTS with Cisco IOS Release 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.</p> <p>Workaround: Disable DMIC on the CMTS.</p>
CSCed71560	<p>A Cisco uBR10000 series router running Cisco IOS Release 12.3 (15)BC1b fails DHCP for customer premises equipment (CPE) inside a Motorola DCT5000 when no bundle entry is found for an incoming DHCP packet.</p> <p>The issue is restricted to only such settop boxes - modems always come online ok on the same Cisco uBR10000 series router and cable line card.</p> <p>Workaround: Follow the following steps:</p> <ol style="list-style-type: none"> <li>1. Feed the failing DCT CPE mac addr to the following CLI: <pre>show ip arp vrf internet CPE mac addr</pre> <p>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.</p> </li> <li>2. To find out offending IP entries in the CMTS bundle table, use the CMTS hidden CLI of: <pre>show int cx/y/z buck rp</pre> <p>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: <pre>clear cable host offending IP's mac addr</pre> </p></li> <li>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.</li> </ol>
CSCed72979	<p>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 <b>hw-module reset</b> command.</p> <p>There are no known workarounds.</p>
CSCed75425	<p>Clearing counters on a Cisco uBR10000 series router can cause SRP interface rate counters to be incorrectly reset to 0.</p> <p>There are no known workarounds.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCed76837	<p>If there are lots of CM/customer premises equipment (CPE) in the line card, 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).</p> <p>The MIB tables are listed below. They are all invoke the same API to get the sorted table which the entry is searched.</p> <p>CISCO-DOCS-EXT-MIB: cdxCmCpeTable,  DOCS-IF-MIB: docsIfCmtsMacToCmTable  DOCS-QOS-MIB: docsQosCmtsMacToSrvFlowTable  CISCO-DOCS-REMOTE-QUERY-MIB: cdrqCmtsCmStatusTable</p> <p>After the fix:</p> <ol style="list-style-type: none"> <li>1. All the SNMP query for above tables will get info from RP/NPE only, so LC will not be affected.</li> <li>2. The SNMP query Get EXACT will have real time response.</li> <li>3. 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.</li> </ol> <p>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.</p> <p>GET NEXT/GET BULK support is back via CSCed90740.</p>
CSCed76871	<p>The CMTS may print the following messages after an extended period of calls which caused by some MTAs sending messages with old gate ID.</p> <p>There is no effect for ongoing calls nor the new calls to be established:</p> <p>Pktcbl(gdb): Fail to find IE, gate=&lt;gateid&gt;  There are no known workarounds.</p>
CSCed79616	<p>Specific running configuration may not be synched to the standby Performance Routing Engine (PRE). After switchover, behavior is cannot be predicted.</p> <p>Workaround: Do not configure the CMTS from multiple VTY sessions.</p>
CSCed83401	<p>This issue is found by reviewing the code. Whether it happens and what form it takes is unknown.</p> <p>There are no known workarounds.</p>
CSCed83593	<p>Dangling DS service flows</p> <p>This issue occurs with LC switchovers.</p> <p>There are no known workarounds.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCed84052	<p>On a Cisco uBR10000 series router, the throughput for a backhaul queue can decrease significantly intermittently. This issue 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).</p> <p>This issue is less of an issue in the production environment where the pair of default queues on the Gigabit Ethernet link are continuously being used and so are going active and inactive. If instead, there are 2 Gigabit Ethernet links with the backhaul routes being equal cost paths, only one queue will be used per Gigabit Ethernet 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.</p> <p>There are no known workarounds.</p>
CSCed86358	<p>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.</p> <p>This issue may occur under the following conditions:</p> <ul style="list-style-type: none"> <li>• Hot Standby Connection-to-Connection Protocol (HCCP) must be configured on the line card</li> <li>• Secondary service flows must be configured via the cable modem config file</li> <li>• 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 deallocated when it goes offline and are the source of the crash.</li> <li>• Performing a “show cable tech” or “show int CableX/Y/Z sid” after the switchover will access the SIDs that were not deallocated and may crash either the card that has become active or, if another switchover is done, the card that is standby.</li> </ul> <p>There are no known workarounds.</p>
CSCed87070	<p>A Cisco uBR10000 series router with MC5x20 BPEs may produce the following error when Spectrum Groups are added:</p> <pre>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</pre> <p>CPU subsequently spikes to 90% mostly in the interrupt context. A reload may be required in order to recover.</p> <p>There are no known workarounds.</p>
CSCed87675	<p>IPM stuck is prematurely triggered, when it is indicated in the overrun register, also punt packets per interface are accounted better.</p> <p>There are no known workarounds.</p>
CSCed87992	<p>Low bandwidth downstream service flows can get more than the configured max_rate if the packet size in the flow is large.</p> <p>Workaround: Configure max_rate to be greater than 100kbps.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCed89815	<p>A bus error occurs on a Cisco router when you enter the <b>trace</b> command, for example, the <b>trace www.a.net</b> command. When you enter the <b>show version EXEC</b> command, the following error messages are displayed:</p> <pre>System returned to ROM by bus error at PC 0XXXXXXXX, address 0YYYYYYYY 0XXXXXXXX represents the program counter at which the router reloads; 0YYYYYYYY represents the address at which the router reloads.</pre> <p>This issue occurs on a Cisco router that runs Cisco IOS Release 12.2(15)BC1 but may also occur in Cisco IOS Release 12.3 or 12.3 T.</p> <p>For more information on bus errors, refer to the following URL:  <a href="http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml">http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml</a></p> <p>There are no known workarounds.</p>
CSCed91422	<p>The RP CPU on a Cisco uBR10000 series router can go to 100% while handling invalid packets being sent from the customer premises equipment (CPE) on the upstream when <b>source-verify</b> or <b>source-verify dhcp</b> is configured.</p> <p>There are no known workarounds.</p>
CSCed91708	<p>On MC520 cable line cards, the input packet rate and input bit rate, as shown in the <b>show interface</b> command, can become very small when the input packet count is greater than 2<sup>31</sup>, 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.</p> <p>There are no known workarounds.</p>
CSCed92381	<p>This issue will happen if each cable interface of a Cable line card does not share the same TEK lifetime.</p> <p>Workaround: Make all cable interfaces of a Cable line card share the same TEK lifetime.</p>
CSCee01374	<p>The Performance Routing Engine (PRE) unexpectedly reloads when multiple simultaneous config sessions are executed using VTY and the Hot Standby Connection-to-Connection Protocol (HCCP) is configured in the cable interfaces.</p> <p>There are no known workarounds.</p>
CSCee01627	<p>In Cisco IOS Release 12.2(15)BC2a and BC2b, on a Cisco uBR10000 series router, for bursty traffic, packets can be erroneously marked as non-conforming even when the average data rate is below the configured max rate.</p> <p>There are no known workarounds.</p>
CSCee02150	<p>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”.</p> <p>It is possible that worms on customer premises equipment (CPE) 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.</p> <p>There are no known workarounds.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCee03345	<p>If on a system with the Hot Standby Connection-to-Connection Protocol (HCCP) configured, the Protect line card unexpectedly reloads 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</p> <p>There are no known workarounds.</p>
CSCee08163	<p>The Performance Routing Engine (PRE) hangs during an N+1 line card switchover with the <b>cable source verify dhcp</b> command enabled. This issue occurs due to a race condition in the code.</p> <p>There are no known workarounds.</p>
CSCee08290	<p>If modems are deleted/reset in bulk using the <b>clear cable modem all delete/reset</b> command, it may cause a CPU-Hog message or may sometimes cause the cable line card to reset.</p> <p>There are no known workarounds.</p>
CSCee11695	<p>When the CMTS is configured with <b>cable source-verify dhcp</b>, and bundling is configured, and ip pkts from customer premises equipment (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.</p> <p>There are no known workarounds.</p>
CSCee13327	<p>Fib index may not be correctly set for DHCP customer premises equipment (CPE) in pxf source-verify tables (affects mainly customers with MPLS VPN and <b>source-verify dhcp</b> configured)</p> <p>The output of <b>show pxf cable source-verify   i sid</b> will show different Fib Index for CM and CPE or multiple entries for the same IP address and SID but different Fib index.</p> <p>Workaround: Do not configure <b>cable source-verify [dhcp]</b>.</p>
CSCee14029	<p>Excessive source verify punts to the RP on the Cisco uBR10000 series router can render the router unusable temporarily.</p> <p>Workaround: Unconfigure source-verify.</p>
CSCee15965	<p>Executing “show srp topology” for a Cisco uBR10000 OC-12 SRP line card gives false “Last received topology pkt” and “Last topology change was” values.</p> <p>This issue occurs when the OC-12 SRP card is on the ring, interface up, transmitting topology packets. No other particular conditions.</p> <p>There are no known workarounds.</p>
CSCee16606	<p>Cable intercept might not send copy of Downstream packets to the collection server, only Upstream packets might appear on the collection server.</p> <p>This issue is seen with the Cisco IOS Release 12.2(15)BC1b image.</p> <p>There are no known workarounds.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCee20385	<p>Under some congestion/traffic conditions, routing updates such as ISIS may get dropped.</p> <p>There are no known workarounds other than to investigate and throttle the traffic conditions causing the congestion.</p>
CSCee20869	<p>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 &amp; ISR context when <b>cable source-verify dhcp</b> and <b>no cable arp</b> is configured.</p> <p>There are no known workarounds.</p>
CSCee21114	<p>When <b>source-verify dhcp</b> and <b>no cable arp</b> is configured, DHCP lease query response for dst address of pkts coming from the back-haul is dropped.</p> <p>The customer premises equipment (CPE) is unreachable from the back-haul until the CPE itself send an ARP or IP packet.</p> <p>Workaround: Do not configure <b>no cable arp</b>.</p>
CSCee22333	<p>Working line-cards may reload during a LC switchover. The number of line-cards that fail is random.</p> <p>There are no known workarounds.</p>
CSCee24107	<p>The slot preference algorithm gives preference to PRE-A to become the active after a reload.</p> <p>This algorithm sometimes was not working, and PRE-B become the active on reload.</p> <p>Workaround: Perform a Performance Routing Engine (PRE) switchover (redundancy force failover) if PRE-B became active.</p>
CSCee24435	<p>After the PXF is reloaded on a Cisco uBR10000 series router, some CMs may get stuck in init(o) or init(t) state.</p> <p>Workaround: Enter <b>clear cable modem mac delete</b> for these CMs.</p>
CSCee24903	<p>CMTS crashes when issuing <b>show hard pxf cpu context</b> command.</p> <p>There are no known workarounds.</p>
CSCee25855	<p>The line card that is becoming active could reload unexpectedly.</p> <p>There are no known workarounds.</p>
CSCee26361	<p>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.</p> <p>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.</p> <p>There are no known workarounds.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCee27549	<p>SNMP query does not detect specific modems via cdxCmCpeCmStatusIndex in the Cisco IOS Release 12.2(15)BC1c. The issue occurs on only a few cable modems on the Cisco uBR10000 chassis.</p> <p>Its noticed that same cable modem, for which snmp poll is failing, appeared under multiple cable interfaces.</p> <p>There are no known workarounds.</p>
CSCee27859	<p>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 line card reload.</p> <p>There are no known workarounds.</p>
CSCee30001	<p>On a system running traffic, a large number of cm_unreg diversions is seen even if all modems are online. The percentage of diversions fluctuates between about 0.1% to 0.6% of traffic. This causes additional RP CPU load of up to 9% (interrupt) with 330,000 pps system throughput.</p> <p>There are no known workarounds.</p>
CSCee31581	<p>Configuring the Hot Standby Connection-to-Connection Protocol (HCCP) on an interface immediately after taking the interface out of shutdown causes the Working interface to be stuck down.</p> <p>Workaround: Delay configuring HCCP until the interface is up or configure HCCP before taking the interface out of shutdown to avoid this issue.</p>
CSCee32609	<p>The CMTS may report a CPU hog error when processing GetBulk SNMP requests.</p> <p>There are no known workarounds.</p>
CSCee32628	<p>The CMTS may report the error below:</p> <pre>%UBR10000-3-NOMEM: Failed to get buffer from flap-list private pool.</pre> <p>There are no known workarounds.</p>
CSCee35423	<p>Performance Routing Engine (PRE) unexpectedly reloads if an interface is shut down and then immediately unconfigure HCCP on it.</p> <p>There are no known workarounds.</p>
CSCee35624	<p>The line card may unexpectedly reload after a N+1 switchover.</p> <p>There are no known workarounds.</p>

Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)

DDTS ID Number	Description
CSCee39458	<p>When configured “snmp-server ifindex persist”, and the line card with less number of downstreams is replaced by the line card with more number of downstreams, SNMP query next entry for the following MIB tables could possibly miss entries.</p> <p>DOCS-QOS-MIB:</p> <ul style="list-style-type: none"> <li>• docsQosPktClassTable,</li> <li>• docsQosParamSetTable,</li> <li>• docsQosServiceFlowTable,</li> <li>• docsQosServiceFlowStatsTable,</li> <li>• docsQosUpstreamStatsTable,</li> <li>• docsQosDynamicServiceStatsTable,</li> <li>• docsQosPHSTable</li> </ul> <p>There are no known workarounds.</p>
CSCee40287	<p>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.</p> <p>Workaround: Wait for all interfaces on the LC to be ready for switchover before issuing CLI switchover.</p>
CSCee41512	<p>The line card in the CMTS may report IPC errors and reload.</p> <p>This happens after a few LC switchovers with BPI+ enabled.</p> <p>There are no known workarounds.</p>
CSCee44564	<p>When entering the <b>cable upstream max-ports</b> command, there is a small probability to get a spurious memory access.</p> <p>The condition <code>_may_</code> possibly result in an unexpected reload, though none has been seen yet.</p> <p>This will be seen only if spectrum management is active at the same time.</p> <p>Workaround: Shut down interface before entering the <b>cable upstream max-ports</b> command.</p> <p>Alternative workaround one: Disable spectrum management before entering the <b>cable upstream max-ports</b> command.</p> <p>Alternative workaround two: Ensure there is no Spectrum Management activity before entering the <b>cable upstream max-ports</b> command.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCee45280	<p>A router may display the following message repeatedly:</p> <pre> SLOT 8/0: Apr 27 16:55:34.715 CST: %UBR10000-3-OVERLAPIP_CM: Interface Cable8/0/3, IP address 10.40.137.175 assigned to CM 0040.7b79.f380 has been reassigned. SLOT 8/1: Apr 27 16:55:59.263 CST: %UBR10000-3-OVERLAPIP_CM: Interface Cable8/1/4, IP address 10.41.4.92 assigned to CM 00a0.731e.645b has been reassigned. SLOT 7/1: Apr 27 16:56:04.326 CST: %UBR10000-3-OVERLAPIP_CM: Interface Cable7/1/2, IP address 10.42.0.212 assigned to CM 0040.7b76.e656 has been reassigned. Apr 27 16:57:18.006 CST: %REDUNDANCY-5-PEER_MONITOR_EVENT: Primary detected a secondary insertion (raw-event=PEER_FOUND(4)) Apr 27 16:57:18.006 CST: %REDUNDANCY-5-PEER_MONITOR_EVENT: Primary detected a secondary insertion (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5)) Apr 27 16:59:48.161 CST: %SYS-3-CPUHOG: Task ran for 4644 msec (102/84), process = REDUNDANCY FSM, PC = 6045A524. -Traceback= 6045A52C 6045A710 604852FC 604850F0 604E5614 604E5688 60478F6C 604597F0 60459D00 6015022C 60145FF8 6014A23C 60F9AA64 6014A5A8 6014AA7C 6014AC1C </pre> <p>This issue occurs on a Cisco uBR10000 router that is running Cisco IOS Release 12.2(15)BC01b.</p> <p>There are no known workarounds.</p>
CSCee46449	<p>Multicast packets punted when destination going out the POS interface.</p> <p>There are no known workarounds.</p>
CSCee47418	<p>If a line-card switchover is performed with at least 3500 modems, 3us3ds service flows, 20-30% modems will go offline during the switchover.</p> <p>Modems will re-range and come back online.</p> <p>There are no known workarounds.</p>
CSCee52001	<p>Under rare circumstances, an ASSERTION FAILED message followed by a reload may be seen on a Cisco uBR10000 series router, 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.</p> <p>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 Performance Routing Engine (PRE).</p> <p>This issue is seen in Cisco IOS Release 12.2(15)BC1, 12.2(15)BC2, and possibly in all Cisco uBR10000 software images.</p> <p>The issue is more likely to occur with small arp timeout values.</p> <p>There are no known workarounds. However, it is recommended not to change the ARP timeout from its default value.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCee53014	<p>A Cisco 10720 router gives an error message when writing crashinfo. The error message is of the following form:</p> <pre>07:15:05: %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level</pre> <p>There are no known workarounds.</p>
CSCee57481	<p>UBR10K-6-CM_INCONSISTENCY messages may be seen on the RP console after a line card failover. This issue is seen if modems on a particular upstream (or downstream) are forced offline and re-range on another upstream (or downstream).</p> <p>There are no known workarounds.</p>
CSCee57955	<p>The CMTS may unexpectedly reload during a N+1 transition.</p> <p>There are no known workarounds.</p>
CSCee60322	<p>When query next entry for object in DOCS-IF-MIB:docsIfCmtsCmStatusTable, possibly no response from SNMP agent. Mibwalk the whole table possibly miss some entries.</p> <p>Workaround: Use get exact to query the entry.</p>
CSCee62732	<p>Call cannot be made if DS slack term exceeded.</p> <p>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:</p> <pre>change ca-config type=DQOS-DS-SLACK-TERM; value=0</pre> <p>However, it is noticed in customer site, that this affects voice quality where choppy voice is heard, and impact service to customer.</p>
CSCee63917	<p>When performing “show run” multiple times, the value displayed for the cable shared secret changes.</p> <p>There is no performance impact, or negative behavior on the Cisco uBR router itself, but some management systems regard this as a configuration change.</p> <p>This issue occurs in all IOS versions on the Cisco uBR10000 series router when “cable shared secret” or “cable secondary-shared secret” are configured.</p> <p>Workaround: Configure the network management tools to ignore the value after “cable shared secret”.</p>
CSCee64987	<p>The <b>Cable Arp Filter</b> commands are not removed from the Protect line after a revert. This has no operational impact on the CMTS.</p> <p>Workaround: If the Protect card is no longer used in a Hot Standby Connection-to-Connection Protocol (HCCP) configuration, manually remove the following commands if they have been inappropriately been left on the Protect line card configuration:</p> <pre>no cable arp filter reply no cable arp filter request</pre>
CSCee65665	<p>The CMTS may display the error below during an N+1 switch over.</p> <pre>GENERAL-3-EREVENT: No current_if_info</pre> <p>There are no known workarounds.</p>

**Table 103**      **Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCee66747	<p>The Hot Standby Connection-to-Connection Protocol (HCCP) may get into an inconsistent state (Protect does not load the Working config completely) if back-to-back switchovers (Protect to Working1 and Working2 to Protect) are performed very quickly (via a cut n paste).</p> <p>There are no known workarounds.</p>
CSCee69887	<p>A dual SRP ring fails to become active completely due to an is-type mismatch. The output of the <b>show clns neighbors</b> command indicates that a certain system interface remains in the Init state indefinitely, although the output of the <b>show ip interface brief</b> command shows that this interface is up.</p> <p>There are no known workarounds.</p>
CSCee69951	<p>The src-verify lease query filtering functionality has the following issues</p> <ol style="list-style-type: none"> <li>1. Can configure threshold for downstream filter to greater than 255 even though it is not supported.</li> <li>2. Counter does not increment with filter threshold is set to 0.</li> <li>3. Clear counters does not clear the filter counters.</li> </ol> <p>There are no known workarounds.</p>
CSCee71684	<p>In certain cases, a classifier entry will not work after a switchover.</p> <p>There are no known workarounds.</p>
CSCee76039	<p>With Cisco IOS Release 12.2(15)BC2d images, encrypted multicast will not work.</p> <p>Workaround: Do not to encrypt multicast traffic.</p>
CSCee78223	<p>If the modem docsis config file is BPI enabled and, if the modem got marked/locked with dynamic-secret. if the modem tries to register again without theft of service, then the modem seems to gets flap continuously.</p> <p>Workaround: Perform a <b>clear cable modem mac-addr lock</b> .</p>
CSCee78261	<p>When CMTS is configured with spectrum group, issue the <b>no cable spectrum-group</b> command introducing some memory leaks. Moreover, the USs in the removed spectrum group have some bogus freq reassigned with 12.3BC image.</p> <p>There are no known workarounds.,</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCee79463	<p>The system can sometimes unexpectedly reload when the following messages flood the screen:</p> <pre>*Jun  8 17:40:15.923: %UBR10000-3-AUTH_INVALID_MESSAGE_AUTHENTICATION_FAILURE: &lt;132&gt;CMTS[DOCSIS]:&lt;66030207&gt; Auth Invalid - Message(Key Request) Authentication Failure . CM Mac Addr &lt;0000.39ef.4a55&gt; *Jun  8 17:40:31.083: %UBR10000-3-AUTH_INVALID_INVALID_KEY_SEQUENCE_NUMBER: &lt;132&gt;CMTS[DOCSIS]:&lt;66030206&gt; Auth Invalid - Invalid Key Sequence Number. CM Mac Addr &lt;0000.3979.c454&gt; *Jun  8 17:40:31.087: %UBR10000-3-AUTH_INVALID_MESSAGE_AUTHENTICATION_FAILURE: &lt;132&gt;CMTS[DOCSIS]:&lt;66030207&gt; Auth Invalid - Message(Key Request) Authentication Failure . CM Mac Addr &lt;0000.3979.c454&gt; *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</pre> <p>There are no known workarounds.</p>
CSCee84392	<p>In a MPLS/VPN environment cable modem using DOCSIS 1.0 becomes unreachable.</p> <p>The customer premises equipment (CPE) attached to it is still reachable.</p> <p>The current issue has been detected while resetting the modem The sub-interface where the MObem is assign to, is configure with <b>cable source-verify dhcp</b> and <b>no cable arp</b>.</p> <p>Workaround: Make sure <b>no cable arp</b> is unconfigured from the sub-interface default is “cable arp”.</p>
CSCee93770	<p>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.</p> <p>Workaround: Hardware Module reset the Protect line card.</p> <p>Alternative workaround: shut/no shut the non-functional interfaces.</p>
CSCef00658	<p>CMTS does not drop DHCP packets that it should for some DHCP packets that have either yiaddr or chaddr as zero IP and mac addr respectively.</p> <p>There are no known workarounds.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCef02178	The default ranging-backoff value should be changed from “auto” to values of 3 6. Workaround: Hard code the ranging-backoff values to 3 6.
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.
CSCef04614	Improve cable modem bringup performance on a Cisco uBR10000 series 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 <b>ip address 10.2.16.1 255.255.255.240</b> 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 issue.
CSCef10097	With Dynamic UGS serv-flows based Voice Calls, on LC switchover the uBR10K-LC could unexpectedly reload. The specifics of problem scenario is: BPI+ is on, a voice call (dynamic serv-flow) gets established and then gets destroyed. An LC switchover here, could unexpectedly reload the LC. The issue does not happen with all voice calls stay active. There are no known workarounds.
CSCef13047	DOCSIS 1.0+ on a Cisco uBR10000 series router running Cisco IOS Release 12.2(15)BC2b drops downstream voice packets resulting in one-way voice. There are no known workarounds.
CSCef18997	Data transmission rate in a downstream direction for 256QAM modulation take place with higher rate than configured in a cable modem profile. This can be observed with following CMTS commands: <ul style="list-style-type: none"> <li>• <b>show interface cable service-flow verbose</b></li> <li>• <b>show cable modem qos verbose</b></li> </ul> This issue has been noticed with MC16E and MC520u cards with FTP and UDP traffic. The issue Problem is specific to Annex A and has not been noticed with 64QAM. 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 Hot Standby Connection-to-Connection Protocol (HCCP) config for RF switch even if there is no RF switch physically present.

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

<b>DDTS ID Number</b>	<b>Description</b>
CSCef24484	<p>Cable modem are associated to wrong sub-interface in a MPLS VPN setup.</p> <p>This issue occurs when 2 DHCP server are defined/reachable from each sub-interfaces networks.</p> <p>Workaround: Clear cable modem xxxx.xxxxx.xxxx del.</p>
CSCef27859	<p>This code improves the modem bringup performance for a Cisco uBR10000 CMTS. This CMTS has much higher number of cable modems on it compared to the Cisco uBR7200 and that is why this code is being committed to take care of the higher modem count.</p> <p>There are no known workarounds.</p>
CSCef28577	<p>Traceback could occur for 1.0+ modem during DSA.</p> <p>There are no known workarounds.</p>
CSCef29003	<p>IOS COPS clients may not interoperate with some COPS servers.</p> <p>If the COPS server send to IOS a COPS message containing an Error Object with an Error-Code in range 12-15, IOS will reject the message. This violates RFC 2748 (see section 2.2.8). There are no known COPS applications at this time that are known to fail due to this issue, but it could affect future (versions of) COPS applications.</p> <p>There are no known workarounds.</p>
CSCef30093	<p>The following error message and traceback occur at the active Performance Routing Engine (PRE), when the standby PRE is loading after an unexpected reload.</p> <pre>Jul 27 07:31:37.911 UTC: %SYS-3-MGDTIMER: Running timer, init, timer = 63093AE0.</pre> <p>The unexpected reload is tracked in a different DDTS (CSCef27187).</p> <p>There are no known workarounds.</p>
CSCef31956	<p>This is a bug to improve reverse arp lookup on the CMTS for modem bringup.</p> <p>There are no known workarounds.</p>
CSCef32610	<p>It is possible to mis-configure the vi connectors in a way that will result in two upstreams using the same connector (without freq stacking).</p> <p>Workaround: Until more checks are added to the code, the user must perform the checks on the virtual connectors to avoid the connectors conflict.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCef35754	<p>IPC communications with a cable line card 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.</p> <pre> Jul 21 02:08:56.212: %C10KEVENTMGR-1-IRONBUS_FAULT: Ironbus Event 5/0 - &lt;Software-Initiated Event&gt;, 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 - &lt;Software-Initiated Event&gt;, 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 </pre> <p>A recoverable ironbus fault must occur on a cable line card subslot. IPC will fail if the Hot Standby Connection-to-Connection Protocol (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.</p> <p>Workaround: Reset the subslot that had the ironbus fault and the IPC connection to the line card will be recovered.</p>
CSCef38356	<p>If the bandwidth command is configured on a cable interface it can cause incorrect bandwidth to be given to the downstream service flows on a Cisco uBR10000 series router.</p> <p>Workaround: Unconfigure <b>bandwidth</b> command from the cable interface.</p>
CSCef42849	<p>Timing violation in PRE2/PRE1 temperature sensor routine.</p> <p>Since the temperature sensor routines violate timing requirements, the temperature reading fails in new device from a new vendor.</p> <p>Workaround: The failure occurs only in new temperature sensor from new vendor.</p> <p> <b>Note</b> All old type of sensors are not effected. No workaround is needed.</p>
CSCef42977	<p>Under heavy loads (around 500 kpps), the Cisco uBR10000 PXF can stop dequeuing packets from the low priority queues (default data queues).</p> <p>Workaround: The issue can be rectified by a PXF reload (microcode reload pxf).</p>
CSCef43462	<p>Unable to obtain SNMP MIB info correctly after a Performance Routing Engine (PRE) switchover, but able to obtain ifDescr correctly. However, some interface info are missing.</p> <p>This issue occurs in PRE redundancy with Cisco IOS Releases 12.2(15)BC2b and 12.2(15)BC2c.</p> <p>Workaround: Reload PRE or enter the <b>cable upstream max-ports</b> command to force the PRE to download the snmpinfo to the cable line card (CLC) automatically.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCef44517	<p>Immediately after booting up, a PRE1 crashes with the following error:</p> <pre>%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</pre> <p>The fault is limited to PRE1 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:</p> <pre>Top Assy. Part Number      : 800-17437-08                                ^^^</pre> <p>Workaround: Upgrade to Cisco IOS Release 12.2(15)BC1e or higher or upgrade to Cisco IOS Release 12.2(15)BC2d or higher.</p>
CSCef46191	<p>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.</p> <p>All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.</p> <p>Cisco will make free software available to address this vulnerability.</p> <p>Workarounds, identified below, are available that protect against this vulnerability.</p> <p>The Advisory is available at <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040827-telnet</a></p>
CSCef49148	<p>On a Cisco uBR10000 series router, after configuring both the primary shared secret and the secondary shared secret on cable interfaces using the <b>cable shared-secret</b> and <b>cable shared-secondary-secret</b> commands, and the length of the secondary shared secret is longer than the primary, the cable line card (MC28C, MC5x20) may reload unexpectedly.</p> <p>There are no known workarounds.</p>
CSCef49769	<p>The 2x8 LC on the Cisco uBR10000 series 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.</p> <p>This can cause box-wide issues as the LC throttles the PXF severely.</p> <p>Workarounds: Reduce load on the affected line card by moving CMs to a different LC. If you have an LCP1 based 2x8 line card, replace with LCP2 Replace 2x8 line card with 5x20 line card.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCef52235	<p>A Cisco uBR10000 series router running either Cisco IOS Release 12.2(15)BC2c or 12.2(15)BC1b will run into the following issues when a 2x8 LC is running at 100% CPU:</p> <ol style="list-style-type: none"> <li>1. No telnet access, only the console port works.</li> <li>2. Modems that are online cannot come back online, the get stuck in init(rc).</li> <li>3. Message that is being seen when the CMTS becomes unreachable:  <pre>%C10KEVENTMGR-1-MINOR_FAULT: PXF DMA Full OCQ Wait Error</pre> </li> <li>4. Traffic slowing down for all the line cards, especially the backhaul interfaces</li> </ol> <p>The issue was seen on a Cisco uBR10000 series router with 16,000 CMs.</p> <p>Workaround: Reduce load on the LC running at 100% CPU.</p> <p>Alternative workaround: Reload the PXF microcode.</p>
CSCef53390	<p>The sample rate range is calculated based on the monitoring duration as compared to the previous (STM1.0) constant range of 10 - 30 minutes. The range is calculated as follows:</p> <ul style="list-style-type: none"> <li>• The maximum memory to be used per line card for STM is 10 MBytes.</li> <li>• The maximum number of modems that can be supported is 6000 per line card. Now, per sample memory consumption is 8 bytes hence approximately, the maximum number of samples that can be allowed are <math>10 * 10^6 / (6 * 10^3 * 2 * 8) \sim 100</math>. Hence, given the duration the sample rate would be calculated as <math>\text{duration} / 100 = \text{sample rate}</math> only if the duration happens to be more than 1440. For monitoring duration less than 1440, the sample rate range would be 10 - 30 minutes.</li> </ul> <p>Hence, with STM 1.0 if someone had the duration as 2 days and the sample rate was 20 minutes, that command would fail when we try to restore that configuration in STM1.1 as now the range would be 28 to 86 minutes. The feature to convert the STM1.0 configuration to STM1.1 was committed through CSCee58978.</p> <p>There are no known workarounds.</p>
CSCef56071	<p>Enforce-rule configured via SNMP is not effective at the CMTS.</p> <p>The same rule when configured thru CLI does not have any issues.</p> <p>There are no known workarounds.</p>
CSCef56516	<p>Signal-to-noise ratio (SNR) values can lower then expected with MC520u card.</p> <p>This issue occurs if virtual connectors 16,17,18,19 are used.</p> <p>There are no known workarounds.</p>
CSCef57375	<p>On a Cisco 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.</p> <p>There are no known workarounds.</p>

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description																				
CSCef58105	<p>Show cable modem offline does not correctly show the previous state of the modem when going through the provisioning steps.</p> <p>There are no known workarounds.</p>																				
CSCef60697	<p>Fix chassis unexpectedly reloads due to acl processing of fragmented packets.</p> <p>The Cisco uBR10000 series router will crash when the RP processor processes a 0th fragmented packet on an interface that has an ACL attached.</p> <p>This issue occurs when an ACL is attached to an interface &amp; the packet is a 0th fragmented packet.</p> <p>There are no known workarounds.</p>																				
CSCef60926	<p>In a 1.0+ redundant environment, if a switchover is issued using the <b>hccp x switch y</b> command, new downstream dynamic service flows are not be established on all new call attempts through the Protect card.</p> <p>There are no known workarounds.</p>																				
CSCef63012	<p>During an N+1 switchover, the following CPUHOG error message may appear at the PROTECTOR cable line card (CLC) and the RP:</p> <pre data-bbox="574 909 1455 957">%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (1200/1160),process = HCCP_DATA_P1.</pre> <p>There are no known workarounds.</p>																				
CSCef65077	<p>The PRE2 FIB code has been modified so that packets with the PUNT adjacency flag now get a new divert-code of PS_DIVERT_CODE_FIB_RP_PUNT.</p> <p>Packets with the RECEIVE adjacency flag continue to get PS_DIVERT_CODE_FIB_RP_DEST, but the RP_DEST divert-code has now been assigned a priority of 5 (instead of zero). The RP_PUNT divert-code gets a priority of zero. The treatment of GLEAN adjacencies remains the same:</p> <table border="1" data-bbox="574 1224 1276 1377"> <thead> <tr> <th>adjacency flag</th> <th>old div-code</th> <th>old priority</th> <th>new div-code</th> <th>new priority</th> </tr> </thead> <tbody> <tr> <td>GLEAN</td> <td>FIB_RP_GLEAN</td> <td>0</td> <td>FIB_RP_GLEAN</td> <td>0</td> </tr> <tr> <td>PUNT</td> <td>FIB_RP_DEST</td> <td>0</td> <td>FIB_RP_PUNT</td> <td>0</td> </tr> <tr> <td>RECEIVE</td> <td>FIB_RP_DEST</td> <td>0</td> <td>FIB_RP_DEST</td> <td>5</td> </tr> </tbody> </table> <p>SNMP and telnet traffic gets the RECEIVE adjacency flag, and will now be diverted with high priority.</p> <p>This DDTS was created when it was shown that on the PRE2, SNMP and telnet traffic timed-out under congestion conditions. Testing shows that the problem has been fixed. See Test-Results and email-trail attachments.</p> <p>There are no known workarounds.</p>	adjacency flag	old div-code	old priority	new div-code	new priority	GLEAN	FIB_RP_GLEAN	0	FIB_RP_GLEAN	0	PUNT	FIB_RP_DEST	0	FIB_RP_PUNT	0	RECEIVE	FIB_RP_DEST	0	FIB_RP_DEST	5
adjacency flag	old div-code	old priority	new div-code	new priority																	
GLEAN	FIB_RP_GLEAN	0	FIB_RP_GLEAN	0																	
PUNT	FIB_RP_DEST	0	FIB_RP_PUNT	0																	
RECEIVE	FIB_RP_DEST	0	FIB_RP_DEST	5																	
CSCef65495	<p>If the bandwidth command is configured on a cable interface it can cause incorrect bandwidth to be given to the downstream service flows on a Cisco uBR10000 series router.</p> <p>Workaround: Unconfigure <b>bandwidth</b> command from the cable interface.</p>																				

**Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)**

DDTS ID Number	Description
CSCef68419	<p>A Cisco uBR 10000 series router running Cisco IOS Release 12.2BC images may crash by a Sgrtrap exception if an extremely low bandwidth value is specified under a Cable Interface:</p> <pre> CMD: 'bandwidth 10 ' 12:01:34 Tue Sep 7 2004 Sep 7 09:01:35.359: %SYS-5-CONFIG_I: Configured from console CMD: 'sho cable modem flap Unexpected exception, CPU signal 5, PC = 0x6012CB08 -Traceback= 6012CB08 6012D65C 603180E0 60318BA0 603063C4 60306878 60315FCC 6050BD68 6050BD4C </pre> <p>There are no known workarounds.</p>
CSCef68700	<p>The active PRE2 (Secondary) crashes with Bus Error Exception and System Switched to standby (Primary) PRE2.</p> <p>There are no known workarounds.</p>
CSCef69368	<p>When toaster VTMS receives excessive OCQ flow off from a line card of to-rp link, it can cause severe performance degradation of VTMS or it can lockup the timing wheel causing VTMS not to service any line card.</p> <p>This issue occurs when excessive OCQ flow off from line card in the presence of over subscription of link.</p> <p>There are no known workarounds.</p>
CSCef70056	<p>After a CLI switch over, customer premises equipment (CPE) devices on the slave interfaces may lose connectivity.</p> <p>Workaround: Reload the CPE device.</p>
CSCef77451	<p>After issuing the test crash command the output pauses before printing out the menu options. When this pause occurs, hitting &lt;Enter&gt; allows the menu be printed and the user to select an option.</p> <p>There are no known workarounds.</p>
CSCef78292	<p>CPUHOG traceback appears on the RP console during switchover.</p> <p>This issue occurs on large-scale systems, &gt;35K CMs, possibly scrypt kiddies.</p> <p>Also, cable bundle has to be configured and switchover has to be configured and performed within this bundle.</p> <p>There are no known workarounds.</p>
CSCef82436	<p>When we have more than 2K modems ranging on an active interface, the standby LC can reload unexpectedly, while synching those ranged SIDs into its inter-db.</p> <p>There are no known workarounds.</p>
CSCef83416	<p>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.</p> <p>This issue occurs in a 2+1 or a larger system. It does not occur in a 1+1 system.</p> <p>Workaround: Disable BPI/PHS.</p>

Table 103 Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)

DDTS ID Number	Description
CSCef83933	LC HA: N+1 using 520U card will not work after switch over when BPI/PHS and Virtual Interface are configured.  There are no known workarounds.
CSCef85824	The router may reload as a result of the following 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.
CSCin54055	DOCSIS1.0 Qos profile created by CM is not seen in the <b>show cable qos profile</b> CLI output after a Performance Routing Engine (PRE) switchover.  There are no known workarounds.
CSCin71529	When the cable QoS permission for the modems is disabled, the qos profile created by the modem may not be removed from the QoS profile table.  Also, if a cable interface is shutdown or if one issues a “clear cable modem cax/y/z all delete” on the CMTS, the qos profile feature gets broken for deletion of qos profiles - the profile should be deleted, but it won't since the internal reference count of the profile is messed up.  There are no known workarounds.
CSCin71861	If 255 customer premises equipment (CPE) devices are configured behind CMs in the system, the primary Performance Routing Engine (PRE) reloads unexpectedly.  Workaround: Configure some small number of allowable CPEs such as 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 reload unexpectedly.  Spectrum management software module is modified to remove the spectrum group in the proper sequence.  There are no known workarounds.
CSCin75900	The networks connected to the customer premises equipment (CPE) router (in case of business customers) become unreachable after a Performance Routing Engine (PRE) switchover if <b>cable source-verify [dhcp]</b> is configured on the CMTS (sub) interface associated with the modem.  There are no known workarounds.
CSCin75998	When both <b>cable tftp-enforce</b> and DMIC CLIs are configured, tftp-enforce may not get the precedence over DMIC.  There are no known workarounds.

**Table 103** *Resolved Caveats for Cisco IOS Release 12.3(9a)BC (continued)*

DDTS ID Number	Description
CSCin76192	Traceback can be observed in an image with a fix for CSCee32628 during flap list aging. There are no known workarounds.
CSCin78666	While doing 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 DOCSIS 1.1 config file is provisioned to the Toshiba modem with BPI+ enabled traffic may get stuck after switchover. There are no known workarounds.
CSCin82407	Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server. Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources. This advisory will be posted to <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050406-xauth">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050406-xauth</a>

## Documentation Updates

### Changes

There are no document updates for this release.

## 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, page 771](#)
- [Platform-Specific Documents, page 771](#)
- [Feature Modules, page 772](#)
- [Cisco Feature Navigator, page 772](#)
- [Cisco IOS Software Documentation Set, page 772](#)

## Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on Cisco.com and the Documentation CD-ROM:

- [Cisco IOS Software Releases 12.3 Mainline Release Notes](#) on Cisco.com at:  
**Cisco IOS Software: Cisco IOS Software Release 12.3 Family: Cisco IOS Software Releases 12.3 Mainline: Release Notes: Cross-Platform Release Notes**

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_release_notes_list.html)



### Note

**Cisco IOS Software Release 12.2 Family: Cisco IOS Software Releases 12.2 Mainline** 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://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>

## 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](#)
- [Cisco CMTS Universal Broadband Router MIB Specifications Guide](#)

On the Documentation CD-ROM:

**Cisco Product Documentation: Broadband/Cable Solutions: Cisco uBR10000 Series Universal Broadband Routers**

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

- [Cisco uBR-RFSW RF Switch Installation and Configuration Guide](#)
- [Cisco uBR-RFSW RF Switch Cabling Instructions](#)
- [Cisco uBR-RFSW RF Switch Regulatory Compliance and Safety Information](#)



### 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/en/US/products/hw/cable/ps2209/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/cable/ps2209/tsd_products_support_series_home.html)

## Feature Modules

Feature modules describe new software enhancements, committed as features, 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.

**Cisco IOS Software: Cisco IOS Software Release 12.3 Family: Cisco IOS Software Releases 12.3 Mainline: Feature Guides**

## 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](mailto: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:

<https://tools.cisco.com/RPF/register/register.do>

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/go/fn>

## 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 the Documentation CD-ROM:

**Cisco IOS Software Configuration: Cisco IOS Release 12.3: Configuration Guides and Command References**

## Release 12.3 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.

**Cisco IOS Software: Cisco IOS Software Release 12.3 Family: Cisco IOS Software Releases 12.3 Mainline: Configuration Guides**

**Cisco IOS Software: Cisco IOS Software Release 12.3 Family: Cisco IOS Software Releases 12.3 Mainline: Command References**

On the Documentation CD-ROM:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Configuration Guides and Command References**

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2008-2011 Cisco Systems, Inc. All rights reserved.



