



# Release Notes for the Cisco 10000 Series Internet Router for Cisco IOS Release 12.2(16)BX1

---

September 24, 2003

These release notes provide information about Cisco IOS Release 12.2(16)BX1, which provides Service Selection Gateway features for the Cisco 10000 series Internet router.

These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode and related documents.

Cisco IOS Release 12.2(16)BX1 is based on the following releases:

- Cisco IOS Release 12.2(16)BX
- Cisco IOS Release 12.2(15)BX
- Cisco IOS Release 12.2(15)BZ
- Cisco IOS Release 12.2(4)BZ1
- Cisco IOS Release 12.0(20)ST for features specific to the Cisco 10000 router
- Cisco IOS Release 12.2B for platform-independent features

To review the release notes for Cisco IOS Release 12.0(20)ST, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/relnote/7000fam/rn120st.htm>

To review the release notes for Cisco IOS Release 12.2, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122reInt/xprn122/index.htm>



---

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

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

# Contents

This document contains the following sections:

- [System Requirements, page 2](#)
- [New Features—Cisco IOS Release 12.2\(16\)BX1, page 2](#)
- [Software Features Supported on the Cisco 10000 Series Router, page 3](#)
- [Limitations and Restrictions, page 4](#)
- [Important Notes, page 6](#)
- [Open Caveats—Cisco IOS Release 12.2\(16\)BX1, page 9](#)
- [Resolved Caveats—Cisco IOS Release 12.2\(16\)BX1 and 12.2\(16\)BX, page 15](#)
- [Other Caveats, page 31](#)
- [Obtaining Documentation, page 32](#)
- [Obtaining Technical Assistance, page 33](#)
- [Obtaining Additional Publications and Information, page 34](#)

## System Requirements

Cisco IOS Release 12.2(16)BX1 requires that you have the performance routing engine (PRE), Part Number ESR-PRE2 installed in the Cisco 10000 chassis. To verify which PRE is installed in the router, use the **show version** command.

## Upgrading to a New Software Release

For specific information about upgrading your Cisco 10000 series router to a new software release, refer to the [Cisco 10000 Series Internet Router Software Configuration Guide](#).

For general information about upgrading to a new software release, refer to the product bulletin [Cisco IOS Upgrade Ordering Instructions](#).

For additional information about ordering Cisco IOS software, refer to the [Cisco IOS Software Releases](#).

## New Features—Cisco IOS Release 12.2(16)BX1

There are no new features in Cisco IOS Release 12.2(16)BX1.

# Software Features Supported on the Cisco 10000 Series Router

Table 1 lists the leased line features based on Cisco IOS Release 12.0(20)ST, and supported in the Cisco 10000 series router.

**Table 1** Software Features Based on Cisco IOS Release 12.0(20)ST

<b>Administration</b>	Cisco Discovery Protocol (CDP) Simple Network Management Protocol (SNMP)
<b>Availability</b>	Route Processing Redundancy Plus (RPR+)
<b>Encapsulations</b>	Ethernet High-Level Data Link Control (HDLC) Point-to-Point (PPP) Multilink Point-to-Point (MLP)
<b>Multiprotocol Label Switching</b>	Multiprotocol Label Switching Virtual Private Network (MPLS/VPN) edge services 802.1q PXF switching for ARPA encapsulation
<b>Multicast Features</b>	Multicast Static Routes Multicast Routing Monitor (MRM)
<b>Multicast Services</b>	Internet Group Management Protocol (IGMP) Protocol-Independent Multicast (PIM) Distance Vector Multicast Routing Protocol (DVMRP) Cisco Group Management Protocol (CGMP) Unidirectional Link Routing (UDLR) Session Directory Protocol (SDP) Multicast Source Discovery Protocol (MSDP) Border Gateway Protocol (BGP)
<b>Routing Protocols</b>	BGP Intermediate System-to-Intermediate System (IS-IS) Open Shortest Path First (OSPF) Interior Gateway Routing Protocol (IGRP) Enhanced Interior Gateway Routing Protocol (EIGRP) Routing Information Protocol (RIP) Policy Based Routing (PBR)
<b>Security Features</b>	Standard and extended access lists Authentication, Authorization, and Accounting (AAA) Kerberos authentication and client support on Telnet Remote Authentication Dial-In User Service (RADIUS) authentication Terminal Access Controller Access Control System Plus (TACACS+)

# Limitations and Restrictions

This section describes limitations and restrictions for the following areas. Be sure to review these limitations and restrictions before you use the Cisco 10000 series router.

- [ssg bind direction Command Not Supported, page 4](#)
- [L2TP Tunnel Authorization, page 4](#)
- [Broadband Aggregation Groups, page 4](#)
- [ATM PXF Queuing, page 4](#)
- [Dynamic Bandwidth Selection, page 5](#)
- [QoS Service Policy on a Virtual Access Interface, page 5](#)
- [CISCO-VPDN-MGMT MIB, page 5](#)
- [AAA Method Lists, page 5](#)
- [Unshaped UBR PVCs, page 5](#)
- [Shaped UBR PVCs, page 5](#)
- [Controlling the Rate of Logging Messages, page 6](#)
- [Testing Performance of High-Speed Interfaces, page 6](#)

## ssg bind direction Command Not Supported

Instead of the **ssg bind direction** command, which will now return an error, use the new **ssg direction** command. See the feature module *SSG Direction Command for Interfaces and Ranges* for more information.

## L2TP Tunnel Authorization

Cisco 10000 router supports Layer 2 Tunneling Protocol (L2TP) tunnel authorization. However, RADIUS does not provide attributes for such parameter values as L2TP tunnel timeouts, L2TP tunnel hello intervals, and L2TP tunnel receive window size. When the Cisco 10000 router does not receive a RADIUS attribute for a parameter, the router uses the default value.

## Broadband Aggregation Groups

Cisco IOS Release 12.2(15)BX or later does not support the configuration of Broadband Aggregation (BBA) groups using RADIUS. You must configure BBA groups manually.

## ATM PXF Queuing

If you intend to disable Asynchronous Transfer Mode (ATM) parallel express forwarding (PXF) queuing, to ensure reliable operation you must enter the **no atm pxf queuing mode** command before you configure any virtual circuits (VCs) on an interface. If you have already configured VCs on an interface and you need to change the mode of ATM PXF queuing, remove the VCs from the configuration and then change the ATM PXF queuing mode.

## Dynamic Bandwidth Selection

The Cisco 10000 series router does not support Dynamic Bandwidth Selection (DBS) on virtual path (VP) tunnels.

## QoS Service Policy on a Virtual Access Interface

If you apply an output Quality of Service (QoS) service policy on a virtual-access interface, and that virtual access interface is L2TP tunneled (when the router is configured as an L2TP network server [LNS], for example) and the service policy indicates that the type of service (ToS) or Differentiated Services Code Point (DSCP) bits should be set (with the **set ip** command, for example), the router sends the packets as-is, without changing the IP Precedence bits or DSCP bits. The outer header gets the correct value, but the inner header is not changed.

## CISCO-VPDN-MGMT MIB

SNMP limits the size of Virtual Private Dialup Network (VPDN) template names to 128 characters. This affects the functionality of the CISCO-VPDN-MGMT MIB. Due to this restriction, if any template name (cvpdnTemplateName) in the cvpdnTemplateTable exceeds 128 characters, you cannot use an SNMP **getmany** request to retrieve any table entries. Instead, you must use individual **getone** requests to retrieve each template name that does not exceed 128 characters. For more information, refer to the [Cisco 10000 Series Internet Router Broadband MIB Specifications Guide](#).

## AAA Method Lists

Cisco IOS Release 12.2(14)BX supports a maximum of 99 AAA method lists. If you configure more than 99 AAA method lists using the **aaa authentication ppp** or **aaa authorization network** command, traceback messages appear on the console.

## Unshaped UBR PVCs

Cisco IOS Release 12.2(15)BX or later supports a maximum of 8000 unshaped unspecified bit rate (UBR) VCs on the OC-12 ATM line card. An unshaped UBR permanent virtual circuit (PVC) is a PVC that has no rate configured on it. You can configure up to 16,000 shaped UBR VCs per port on the OC-12 line card if you configure the VCs with a shaped rate of less than 299 Mbps.

## Shaped UBR PVCs

The Cisco 10000 series router does not support shaped UBR in low VC mode.

## Controlling the Rate of Logging Messages

It is important that you limit the rate that system messages are logged by the Cisco 10000 series router. This helps to avoid a situation in which the router becomes unstable and the CPU is overloaded. To control the output of messages from the system, use the **logging rate-limit** command.

We recommend that you configure the **logging rate-limit** command as follows:

```
Router(config)# logging rate-limit console all 10 except critical
```

This rate-limits all messages to the console to 10 per second, except for messages with critical priority (level 3) or greater.

For more information on the **logging rate-limit command**, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

## Testing Performance of High-Speed Interfaces

Cisco IOS software running on the Cisco 10000 series router has multiple queues for all classes of traffic over high-speed interfaces. The software selects a queue based on the source and destination address of the packet. This ensures that a traffic flow always uses the same queue and the packets are transmitted in proper order.

When the Cisco 10000 series router is installed in a real network, the high-speed interfaces work efficiently to spread traffic flow equally over the queues. However, using single traffic streams in a laboratory environment might result in less-than-expected performance.

Therefore, to ensure accurate test results, you should test the throughput of the gigabit Ethernet, Packet Over SONET (POS), or ATM uplink with multiple source or destination addresses.



Tip

---

To determine if traffic is being properly distributed, use the **show pxf cpu queue** command.

---

## Important Notes

This section provides important information about the following items for Cisco IOS Release 12.2(16)BX1:

- [Provisioning for Scaling, page 6](#)
- [Enhancing Scalability of Per-User Configurations, page 7](#)
- [Inserting a New Line Card, page 9](#)

## Provisioning for Scaling

The following configuration parameters enhance scalability on the Cisco 10000 series router:

- [PPPoA Sessions with IP QoS Static Routes, page 7](#)
- [AAA Authentication on the NME Port, page 7](#)
- [Call Admission Control, page 7](#)

To configure the Cisco 10000 series router for high scalability, be sure to configure the configuration parameters as described in the sections that follow.

For more information, refer to the [Cisco 10000 Series Internet Router Broadband Aggregation Configuration Guide](#).

## PPPoA Sessions with IP QoS Static Routes

To scale to 32,000 PPP over ATM (PPPoA) sessions with IP QoS enabled, you must limit the number of IP QoS static routes to 4,000 unidirectional QoS static routes.

## AAA Authentication on the NME Port

If you use AAA authentication on the Network Management Ethernet (NME) port, set both the in and out interface hold queues to 4096. For example:

```
Router(config)# int fa 0/0/0
Router(config-if)# hold-queue 4096 in
Router(config-if)# hold-queue 4096 out
```

## Call Admission Control

We recommend that you set the Call Admission Control (CAC) to a maximum of 95. For example:

```
Router(config)# call admission limit 95
```

## Enhancing Scalability of Per-User Configurations

To enhance scalability of per-user configurations without changing the router configuration, use the **ip:vrf-id** and **ip:ip-unnumbered** RADIUS attributes. These per-user vendor specific attributes (VSAs) are used to map sessions to VPN routing and forwarding (VRF) and IP unnumbered interfaces. The VSAs apply to virtual access subinterfaces and are processed during PPP authorization.

In releases prior to Cisco IOS Release 12.2(16)BX1, the **lcp:interface-config** RADIUS attribute is used to map sessions to VRFs. This per-user VSA applies to any type of interface configuration, including virtual access interfaces. Valid values of this VSA are essentially any valid Cisco IOS interface command; however, not all Cisco IOS commands are supported on virtual access subinterfaces. To accommodate the requirements of the **lcp:interface-config** VSA, the per-user authorization process forces the Cisco 10000 router to create full virtual access interfaces, which consume more memory and are less scalable.

In Cisco IOS Release 12.2(16)BX1 and later releases, the **ip:vrf-id** is used to map sessions to VRFs. Any profile that uses the **ip:vrf-id** VSA must also use the **ip:ip-unnumbered** VSA to install IP configurations on the virtual access interface that is to be created. PPP that is used on a virtual access interface to be created requires the **ip:ip-unnumbered** VSA. An Internet Protocol Control Protocol (IPCP) session is not established if IP is not configured on the interface. You must configure either the **ip address** command or the **ip unnumbered** command on the interface so that these configurations are present on the virtual access interface that is to be created. However, specifying the **ip address** and **ip unnumbered** commands on a virtual template interface is not required because any pre-existing IP configurations are removed when the **ip:ip-vrf** VSA is installed on the virtual access interface. Therefore, any profile that uses the **ip:vrf-id** VSA must also use the **ip:ip-unnumbered** VSA to install IP configurations on the virtual access interface that is to be created.

These per-user VSAs can be applied to virtual access subinterfaces; therefore, the per-user authorization process does not require the creation of full virtual access interfaces, which improves scalability.

## Setting VRF and IP Unnumbered Interface Configurations in User Profiles

Although the Cisco 10000 router continues to support the **lcp:interface-config** VSA, the **ip:vrf-id** and **ip:ip-unnumbered** VSAs provide another way to set the VRF and IP unnumbered interface configurations in user profiles. The **ip:vrf-id** and **ip:ip-unnumbered** VSAs have the following syntax:

```
Cisco:Cisco-AVpair = "ip:vrf-id=vrf-name"
Cisco:Cisco-AVpair = "ip:ip-unnumbered=interface-name"
```

You should specify only one **ip:vrf-id** and one **ip:ip-unnumbered** value in a user profile. However, if the profile configuration includes multiple values, the Cisco 10000 router applies the value of the last VSA received, and creates a virtual access subinterface. If the profile includes the **lcp:interface-config** VSA, the router always applies the value of the **lcp:interface-config** VSA, and creates a full virtual access interface.

Whenever you specify a VRF in a user profile, but you do not configure the VRF on the Cisco 10000 router, in Cisco IOS Release 12.2(15)BX, the router accepted the profile. However, in Cisco IOS Release 12.2(16)BX1 and later releases, the router rejects the profile.

## Setting VRF and IP Unnumbered Interface Configuration in a Virtual Interface Template

You can specify one VSA value in the user profile on RADIUS and another value locally in the virtual template interface. The Cisco 10000 router clones the template and then applies the values configured in the profiles it receives from RADIUS, resulting in the removal of any IP configurations when the router applies the profile values.

## Redefining User Profiles to Use the ip:vrf-id and ip:ip-unnumbered VSAs

The requirement of a full virtual access interface when using the **lcp:interface-config** VSA in user profiles can result in scalability issues, such as increased memory consumption. This is especially true when the Cisco 10000 router attempts to apply a large number of per-user profiles that include the **lcp:interface-config** VSA. Therefore, when updating your user profiles, we recommend that you redefine the **lcp:interface-config** VSA to the scalable **ip:vrf-id** and **ip:ip-unnumbered** VSAs.

[Example 1](#) shows how to redefine the VRF named *newyork* using the **ip:vrf-id** VSA.

### Example 1 Redefining VRF Configurations

```
Change:
Cisco:Cisco-AVpair = "lcp:interface-config=ip vrf forwarding newyork"

To:
Cisco:Cisco-AVpair = "ip:vrf-id=newyork"
```

[Example 2](#) shows how to redefine the Loopback 0 interface using the **ip:ip-unnumbered** VSA.

**Example 2 Redefining IP Unnumbered Interfaces**

Change:

Cisco: Cisco-Avpair = "lcp:interface-config=ip unnumbered Loopback 0"

To:

Cisco: Cisco-Avpair = "ip:ip-unnumbered=Loopback 0"

## Inserting a New Line Card

Unlike other Cisco routers, if you insert a new or different line card into a Cisco 10000 chassis slot that previously had a line card installed, the line card initially reports that it is administratively up.

## Open Caveats—Cisco IOS Release 12.2(16)BX1

Table 2 describes Open Caveats in Cisco IOS Release 12.2(16)BX1.

**Table 2 Open Caveats in Cisco IOS Release 12.2(16)BX1**

Caveat	Description
CSCdy79740	<p>If 32,000 PPPoA sessions, 99 VRFs, RADIUS authentication, and the <b>per vrf aaa case</b> command are configured on the Cisco 10000 series router, and you insert or remove a line card, the PPPoA sessions disconnect within 45 seconds of the online insertion and removal (OIR) event. When this happens, the following traceback message might appear on the console:</p> <pre>[%IPRT-4-ROUTECOUNTNEGATIVE]</pre> <p><b>Workaround:</b> None.</p>
CSCea35508	<p>The throughput of Frame Relay traffic might be up to 5 percent lower than the maximum possible throughput.</p> <p><b>Workaround:</b> None.</p>
CSCea37019	<p>The Cisco 10000 series router displays a bus fault error when Automatic Protection Switching (APS) is configured on the OC-12 ATM line card.</p> <p><b>Workaround:</b> None.</p>
CSCea37038	<p>If APS is configured using the <b>aps force atm slot/subslot/port from protect</b> command on the 4-port OC-3 line card or the single-port OC-12 ATM line card, and a signal failure is received on the port of either line card, the output of the <b>show interface atm slot/subslot/port</b> command might indicate the interface is up instead of down.</p> <p><b>Workaround:</b> Clear the force state as soon as the port has been designated as working, by entering the <b>aps clear atm slot/subslot/port</b> command.</p>
CSCea37133	<p>When you configure APS switchover on the 4-port OC-3 ATM line card, entering the <b>show controller atm slot/subslot/port</b> command for the ATM port displays a signal degrade status for both the protection port and the working port.</p> <p><b>Workaround:</b> Wait more than 2 minutes to allow the signal degrade status to clear or use the <b>aps signal-degrade BER threshold 6</b> command or the <b>aps signal-degrade BER threshold 7</b> command for the ATM interface.</p>

Table 2 Open Caveats in Cisco IOS Release 12.2(16)BX1 (continued)

Caveat	Description
CSCea45943	<p>In a Cisco 10000 chassis with redundant PREs, after a switchover from the primary PRE to the secondary PRE, the traffic rate of the single-port OC-12 ATM line card is low.</p> <p><b>Workaround:</b> None.</p>
CSCea46149	<p>If you connect a test analyzer to the 6-port channelized T3 line card, and you configure a T1 under a T3 controller, and the line card and the test analyzer are both set to Extended Superframe (ESF) framing, the T1 does not start up.</p> <p><b>Workaround:</b> None.</p>
CSCea52741	<p>If the Cisco 10000 series router reloads unexpectedly, any On-Demand Address Pools (ODAP) subnets allocated from the Cisco Network Registrar (CNR) remain marked as Leased (at the CNR).</p> <p><b>Workaround:</b> There is currently no workaround to this problem. However, if this should occur, the subnets are released when the Lease time expires, or they may be released manually through the CNR Command Line Interface (CLI).</p>
CSCea66654	<p>Channelized interfaces with access control lists (ACLs) configured might show an incorrect ACL status even after the ACL is removed from the interface by entering the <b>no ip access acl-name</b> command. This occurs if the interface is rechannelized and the removed ACL is reconfigured on the interface.</p> <p><b>Workaround:</b> None.</p>
CSCea67815	<p>When you disable 32,000 sessions over 10,000 L2TP tunnels on a Cisco 10000 series router configured as an LNS with RADIUS AAA accounting enabled, the router might terminate the remaining sessions due to the overwhelming number of RADIUS records generated by this event. If this occurs, the following message might appear on the console:</p> <pre>%ALIGN-3-TRACE</pre> <p><b>Workaround:</b> None.</p>
CSCea70951	<p>A memory allocation error occurs when you attempt to scale a large number of users (for example, 4000 PPPoA Service Selection Gateway [SSG] sessions). All of the connections are established and the <b>show ssg</b> command displays all of the sessions as logged in and active. However, when sessions are dropped, a memory allocation error appears.</p> <p><b>Workaround:</b> None.</p>
CSCea72016	<p>The channelized OC-12 line card undergoes a watchdog reset when unconfiguring six channelized OC-12 line cards set up with 768 T1s each. This occurs only with a very specific large channelized card setup. This does not occur with five or less channelized OC-12 line cards.</p> <p><b>Workaround:</b> Unconfigure fewer OC-12 channelized interfaces at one time.</p>

Table 2 Open Caveats in Cisco IOS Release 12.2(16)BX1 (continued)

Caveat	Description
CSCea73477	<p>Packet counters and debug messages on the Cisco 10000 series router cannot be used to accurately count or view Interim Local Management Interface (ILMI) keepalive messages. This is because basic ILMI configurations generate bursts of ILMI transactions between the Cisco 10000 series router and adjacent ATM switches.</p> <p>For example, if you connect an OC-3 ATM line card that is installed in a Cisco 10000 series router to a Cisco LS1010 ATM switch, and you enable debugging using the <b>debug atm ilmi</b> command, the packet counters for the ILMI PVC increment to match the bursts of packets.</p> <p><b>Workaround:</b> There is currently no workaround for this problem. However, this problem does not affect the performance or operation of the router.</p>
CSCea77321	<p>If the primary PRE fails, and the primary PRE switches over to the secondary (redundant) PRE, ODAP subnets that had been allocated to the previously active primary PRE remain marked as Leased by the Access Registrar (AR)</p> <p><b>Workaround:</b> Release the sessions associated with the subnets at the AR.</p>
CSCea78861	<p>If you enter the <b>ip verify unicast rpf</b> command for a virtual template, the calls-per-second rate is reduced.</p> <p><b>Workaround:</b> There is currently no workaround for this problem. However, this problem only reduces the calls-per-second rate and does not affect the performance of the router.</p>
CSCea78890	<p>If you perform a <b>tftp copy</b> of a running configuration greater than 5 MB to a trivial file transfer protocol (TFTP) server, the copy fails.</p> <p><b>Workaround:</b> Copy the running configuration to the bootflash and then copy the configuration from the bootflash to the TFTP server.</p>
CSCea81015	<p>If you configure the management Ethernet port (fastethernet 0/0/0) on the PRE (Part Number ESR-PRE2) front panel using the <b>ip address dhcp</b> command, the port does not acquire an IP address.</p> <p><b>Workaround:</b> Configure the fastethernet 0/0/0 interface with a static IP address.</p>
CSCea82309	<p>If you open two configuration sessions on the PRE (Part Number ESR-PRE2) from two console devices, a failure message appears on the console devices stating that simultaneous configuration is not supported.</p> <p><b>Workaround:</b> None.</p>
CSCeb01499	<p>The following traceback message displays in the log after you enter the <b>hardware subslot shutdown, no card</b>, and <b>no hardware subslot shutdown</b> or <b>card 24che1t1 mode t1</b> commands:</p> <pre>May 2 23:31:53: %IPCGRP-3-SYSCALL: System call for command 409 (slot4/0) : ipc_send_rpc_blocked failed (Cause: retry queue flush) -Traceback= 6046B1EC 6046B4C0 6046BD5C May 2 23:31:54: %IPCOIR-4-REPEATMSG: IPC handle already exists for 4/0</pre> <p><b>Workaround:</b> None.</p>
CSCeb08194	<p>When SSG traffic is redirected because users are not authorized for services, CPU usage is high and throughput is limited.</p> <p><b>Workaround:</b> None.</p>

**Table 2** Open Caveats in Cisco IOS Release 12.2(16)BX1 (continued)

Caveat	Description
CSCeb17086	Traceback messages appear while configuring static multicast routes. <b>Workaround:</b> None.
CSCeb21692	A client is unable to ping the SSG access side downlink interface. This occurs when an SSG interface is configured as a downlink interface and routing with bridged encapsulation is configured. <b>Workaround:</b> This occurs when a client is not authenticated and the client tries to ping the SSG downlink interface. After a client is authenticated, the client can ping the SSG downlink interface.
CSCeb26165	While the Cisco 10000 series router terminates PPP sessions and uses RADIUS accounting, the router generates both Accounting-Stop and Accounting-Off messages when you enter the <b>reload</b> command. <b>Workaround:</b> None.
CSCeb33056	The Cisco 10000 series router frequently displays the following interprocess communications (IPC) queue full message:  00:15:49: %IPGRP-6-NBLKCMD_Q_FULL: Nonblocking IPC command queue full (60 commands) <---  <b>Workaround:</b> None.
CSCeb35104	Configurations with a very large number of subinterfaces (for example, 32,000) might experience slow PPP over Ethernet over ATM (PPPoEoA) session clearing. <b>Workaround:</b> None.
CSCeb36330	When a range of VCs are configured for autoprovisioning, if you shut down one of the VCs in the range by using the <b>pvc-in-range</b> command, the following message scrolls on the console until you start the VC again:  Jun 11 09:09:33.215: %ATM-5-UPDOWN: Interface ATM3/0/0.100, Changing autovc 3/101 to ADMIN_DOWN  <b>Workaround:</b> None.
CSCeb38277	When an ATM interface is configured as unnumbered, the Cisco 10000 series router does not forward routed bridge encapsulation (RBE) traffic to RBE clients. <b>Workaround:</b> None.
CSCeb41285	The Cisco 10000 series router does not create the virtual access interface (VAI) if the RADIUS user profile includes Frame-Compression attribute-value pair (AVP). If the AVP for compression is removed from the user profile, the router creates the VAI. <b>Workaround:</b> Do not specify framed-compression none in RADIUS profiles.
CSCeb42938	The following traceback message randomly appears:  00:48:42: %AAA-3-BADMETHOD: Cannot process authorization method 1635568848 -Process= "AAA Server", ipl= 0, pid= 58 -Traceback= 603B6A1C 603AFE24 603B0C58 603B0D78  <b>Workaround:</b> None.

Table 2 Open Caveats in Cisco IOS Release 12.2(16)BX1 (continued)

Caveat	Description
CSCeb48677	<p>Nested policies configured on the main interface of the Gigabit Ethernet (GE) line card do not work. Nested policies configured on GE subinterfaces do work properly.</p> <p><b>Workaround:</b> None.</p>
CSCeb49776	<p>Multiple memory leaks occur while testing the Cisco IOS Release 12.2(16)BX image.</p> <p><b>Workaround:</b> None.</p>
CSCeb51308	<p>When 61,500 PPPoEoA sessions are active and SNMP is running in the background, executing the <b>show adjacency</b> command causes the following traceback message to appear:</p> <pre>05:21:32:%SYS-3-CPUHOG:Task ran for 4120 msec (464/222), process = Virtual Exec, PC = 604F8360.</pre> <p><b>Workaround:</b> None.</p>
CSCeb51344	<p>RADIUS configurations that use <b>lcp</b> in the VSAs are not usable when they are downloaded and are to be VRF-aware on the Cisco 10000 series router. When downloading routes from RADIUS that are configured using Internet Engineering Task Force (IETF) attributes, sessions are established as expected and the routing table lists the routes as per-user routes.</p> <p><b>Workaround:</b> None.</p>
CSCeb52243	<p>On the 8-port DS3/E3 ATM line card, F5 Operation, Administration, and Maintenance (OAM) Rate Limiting does not properly drop the OAM cells that exceed the rate limit.</p> <p><b>Workaround:</b> None.</p>
CSCeb53208	<p>The Cisco 10000 router creates PPP sessions without allocating a virtual circuit connection identifier (VCCI).</p> <p><b>Workaround:</b> None.</p>
CSCeb53344	<p>During sweep ping testing of the 8-port DS3/E3 line card, a single ping failure occurs.</p> <p><b>Workaround:</b> None.</p>
CSCeb53474	<p>With TACACS configured on the Cisco 10000 series router, the secondary PRE (Part Number ESR-PRE2) console attempts TACACS authentication using the Fa0/0/0 interface. Before notifying the user that the secondary console is unavailable, the secondary PRE incorrectly attempts to contact the TACACS server for user authentication. The secondary PRE should not attempt to contact the TACACS server or it should try to contact the TACACS server using the primary PRE.</p> <p><b>Workaround:</b> None.</p>
CSCeb54544	<p>When a VC class has an autopp encapsulation configured, if you create a new VC class by entering the <b>vc-class</b> command or you make changes to an existing VC class, the Cisco 10000 series router deletes all of the VCs that are included in the VC class with autopp encapsulation and then creates the VCs again.</p> <p><b>Workaround:</b> None.</p>

Table 2 Open Caveats in Cisco IOS Release 12.2(16)BX1 (continued)

Caveat	Description
CSCeb54587	<p>When a service policy is configured in a virtual template, the following error message appears as the session is being established:</p> <pre> Couldn't get main subinterface's tt_if_info from c10k_check_should_policy_be_applied </pre> <p>This is not an error condition. This message is an obsolete message. The service policy is applied as expected.</p> <p><b>Workaround:</b> None.</p>
CSCeb55625	<p>When you hot swap an 8-port DS3/E3 ATM line card with a 1-port OC-12 POS line card, the following traceback message appears. The Cisco 10000 series router properly provisions the 1-port OC-12 POS line card.</p> <pre> *Jul  3 08:48:24.990:%C10K-3-LC_ERR:Slot [8/0] loc12pos-1 process_oir_set_image_message:cardtype 0x0 not 0x1. *Jul  3 08:48:24.990:%IPCOIR-3-LOADER_SERVER_FAIL:Remote server refused to load slot 8/0 *Jul  3 08:48:25.066:%GENERAL-3-EREVENT:c10k_icmp_ipaddr_setup:No c10k_tt_hwsb -Traceback= 60BDBB34 60B8B304 60B8BCFC 60B8B664 605171CC 6051A984 60381210 603813F4 6007938C 6048DA04 </pre> <p><b>Workaround:</b> To prevent the traceback message from occurring, first remove the 8-port DS3/E3 ATM line card from the chassis and then remove the line card from the configuration using the <b>no card slot#</b> command. You can then insert the 1-port OC-12 POS line card into the chassis.</p>
CSCeb58934	<p>After you issue a <b>debug qos-set</b> command, the debug output of the command is not disabled with the <b>no debug all</b> command and it does not appear in the output of the <b>show debug</b> command.</p> <p><b>Workaround:</b> Use the <b>no debug qos-set</b> command to disable debugging.</p>
CSCeb59318	<p>When a user's profile on the RADIUS system includes the AVP attribute Framed-Compression = None, the virtual interface will create on the router. The fix that enables it (CSCeb41285) caused another issue. Currently, when the router negotiates the parameters for the session with the RADIUS server, a Full VAI is being created if Framed-Compression AVP exists in the user profile.</p> <p><b>Workaround:</b> Remove the offending AVP (Framed-Compression = None) and set the default setting of RADIUS to No Compression.</p> <p>If the RADIUS server supports both dial-up customers (modem) and broadband users, there is a chance that Van Jacobson (VJ) compression is enabled by default on the server. Since the router does not support VJ compression on PPP over X (either Ethernet or ATM) (PPPoX), there is a need to disable the compression for the broadband user, until a fix is present for the router. If RADIUS supports only broadband users and it is set by default to support VJ compression in PPP packets, it is recommended at this point to set the default compression behavior to none.</p>

**Table 2** Open Caveats in Cisco IOS Release 12.2(16)BX1 (continued)

Caveat	Description
CSCeb77168	<p>If two users are logged into the router, and one user begins a save of the system configuration to removable flash media while another user initiates a system reload, the configuration file on the removable media becomes corrupted and no file operations are possible on the file (erase, copy, and overwrite do not work).</p> <p><b>Workaround:</b> Reformat the removable media after saving any pertinent files to another location, or delete the corrupted file from a PC.</p>
CSCeb77178	<p>If you want to store a configuration locally on removable flash media disk0 and you are using the boot config statement and the boot config environment variable to point to the same configuration file on disk0, the file is not automatically synchronized to disk0 on the redundant PRE (sec-disk0). In the event of a failure, the backup PRE would not have access to the current configuration file.</p> <p><b>Workaround:</b> Store the configuration file on a remote server. Or manually copy the configuration file stored on disk0 to sec-disk0 whenever a configuration change is made.</p>
CSCec34475	<p>If you load a Field Diagnostics image from disk0, the router could crash.</p> <p><b>Workaround:</b> Load from tftp or bootflash instead.</p>
CSCin46447	<p>When you disable SSG traffic policing on the router by entering the <b>no ssg qos police user</b> and the <b>no ssg qos police session</b> commands, the router continues to police the traffic for the existing host/connection.</p> <p><b>Workaround:</b> None.</p>

## Resolved Caveats—Cisco IOS Release 12.2(16)BX1 and 12.2(16)BX

This section contains information on resolved caveats:

- [Resolved Caveats in Cisco IOS Release 12.2\(16\)BX1, page 15](#)
- [Resolved Caveats in Cisco IOS Release 12.2\(16\)BX, page 28](#)

### Resolved Caveats in Cisco IOS Release 12.2(16)BX1

This section describes caveats that were fixed in Cisco IOS Release 12.2(16)BX1.

#### CSCdy78477

Frame relay interface statistics were not correctly updated under certain conditions:

- The router had received keepalive packets for a period of time.
- The interface was configured with the **no keepalive** command.
- Another router pinged the router. Ping packets are not counted until they are higher than the number of keepalive packets received.

This problem has been fixed.

**CSCdz02843**

For a multilink interface, after issuing a **shut** or **no shut** command, the output statistics could show very large values. This problem has been fixed.

**CSCdz69906**

Stac and TCP header compression were not negotiated when specified in the framed-compression attribute in the AAA message. The attributes were retrieved successfully from the AAA message, but negotiation did not take place. This problem has been fixed.

**CSCdz72406**

On a GigE interface card, sometimes output bytes were not counted correctly so the output counter values were low. This problem was fixed.

**CSCdz76411**

For the **show route-map** [*policy-name*] PBR command, the packet/byte counts for all of the route-maps in each PBR policy were displayed shifted down one route-map. In other words, the display for the first route-map of each PBR policy displayed as zeros, and the counts for route-map N of a PBR policy showed up in the display for route-map N+1 of that policy. This problem was fixed.

**CSCea15720**

A configuration download through TFTP could cause a router crash. The Cisco router could reload during the bootup process because of insufficient memory. When this situation occurred, the router generated messages similar to the following:

```
current memory block, bp = 0x63903D80, memory pool type is Processor
data check, ptr = 0x63903DA8
bp->next(0x605C57C0) not in any mempool
previous memory block, bp = 0x200039E1, memory pool type is Processor
data check, ptr = 0x20003A09
%SYS-3-BADMAGIC: Corrupt block at 63903D80 (magic 61DEC941)
```

This symptom was observed when all of the following conditions were present:

- The network configuration contained ATM PVC configurations.
- The router was configured to retrieve its configuration from a TFTP server.
- The first attempt to make such a retrieval failed.

This problem was fixed.

**CSCea27261**

The network access server (NAS) sent an unwanted access request for PPP termination aggregators (PTAs). When you configured VPDN with RADIUS, a double RADIUS lookup occurred. This decreased performance on a RADIUS server with a large number of additional RADIUS requests. This problem was fixed.

**CSCea30354**

When the 8-port DS3/E3 ATM line card was configured for DS3 add/drop multiplexer (ADM) or DS3 physical layer convergence procedure (PLCP) digital signal cross-connect level 3 (DSX3) mode, and the line card was connected back-to-back with another 8-port DS3/E3 ATM line card, the DS3/E3 ATM interface on the first line card counted a large quantity of 00F events when you shut down the interface on the far-end ATM device. This problem was fixed.

**CSCea34048**

AAA messages needed an additional per-user flag to distinguish between per-user that can work on a subinterface vaccess and per-user needing full vaccess. For example, the compression attribute was supported only for full vaccess. This flag was added.

**CSCea41145**

The output of the **show vpdn tunnel summary** command failed to display tunnels that have a no-session timeout (set using the **l2tp timeout no-session timeout never** command). This problem was fixed.

**CSCea41221**

Executing the **show vpdn** command caused a spurious access error message to be printed to the console port. This problem was fixed.

**CSCea50008**

When the power cord was unplugged, a Power Entry Module (PEM) did not generate a syslog message. The problem has been fixed.

**CSCea53877**

When the Cisco Networking Services (CNS) configuration agent was used to programmatically apply a configuration, the configuration failed and a failure message was published as a `cisco.mgmt.cns.config.failure`. The failure occurred when the secondary PRE card was up and available for hot standby. This problem has been fixed.

**CSCea59894**

On the 8-port DS3/E3 ATM line card, ILMI discovery was not complete when the line card was operating in the DS3 ADM and DS3 PLCP DSX3 modes. The ILMI state remained in the WaitDevType state and the line card did not discover the adjacent ATM switch information. When operating in the E3 ADM and E3 PLCP DSX3 modes, the line card did properly discover the adjacent ATM switch values. This problem no longer exists in this release (it is not reproducible).

**CSCea65080**

A spurious access from an `sss_pm_set_active_key_string` was experienced on a node route processor 2 (NRP2). This problem was fixed.

**CSCea66307**

When a large number (for example, 30,000) of established PPP sessions terminate at the same time, the Cisco 10000 series router could exhaust I/O memory. This caused a loss of other services such as maintaining L2TP tunnels and dropping AAA accounting requests to the RADIUS server. This problem has been fixed.

**CSCea67485**

If you tried to configure 1000 ATM PVCs on a router, you could see failure messages on the secondary Route Processor (RP), even though there was not a failure. This problem has been fixed.

**CSCea69541**

The command **radius-server source-ports 1645-1646** was not displayed in the configuration and therefore had no effect when the router was rebooted. The command is necessary to interoperate with certain vendors' voice gateway RADIUS billing solutions. The workaround was to reconfigure the command after the router has rebooted. This problem has been fixed.

**CSCea82805**

Deleted redundant code from the CSCea59464 fix.

**CSCeb03164**

A memory leak could occur during the PPP events process when PPP was configured on a router. This problem was fixed.

**CSCeb08211**

When a Cisco Router was initiating a PPP disconnect by sending a terminate request, the router sometimes did not wait for the acknowledgment before disconnecting the call. This problem was fixed.

**CSCeb17467**

A Cisco router could reload when BGP was configured to carry Virtual Private Network version 4 (VPNv4) routes. This symptom was observed when VPNv4 import processing occurred simultaneously with a BGP neighbor reset, for example, when a VRF instance was configured and you entered the **clear ip bgp \*** privileged EXEC command. This problem was fixed.

**CSCeb26162**

In some cases, while the Cisco 10000 series router terminated PPP sessions, the router delayed the transmission of the RADIUS Accounting-On message for too long, thus clearing the accounting data on the RADIUS server about the sessions that were already established. This problem has been fixed.

**CSCeb28546**

The **rlogin trusted-remoteuser-source** and **rlogin trusted-localuser-source** configurations, used for sending authenticated usernames to the rlogin connection, did not work if **aaa new-model** was also in use. This problem has been fixed.

**CSCeb30288**

The Cisco 10000 series router could delay executing the **reload** command if AAA accounting was configured. During this time packets were *not* forwarded. This problem has been fixed.

**CSCeb30426**

Field Diagnostics could not detect 8-port Fast Ethernet line cards when the card was shut down. This problem has been fixed. With the fix, the card is detectable when it is shut down.

**CSCeb31498**

When DBS was enabled on a VC class, DBS failed and displayed the following error message:

```
Jun  5 13:21:19.200: %C10K DBS: validate_params() 2/111, vcd 11, QoS type 5, PCR 50, SCR 38
```

```
Jun  5 13:21:19.200: %C10K DBS: validate() QoS update rejected PVC 2/111 on VP tunnel
```

This problem has been fixed.

**CSCeb36225**

The NAS sent a RADIUS Access-Request for a domain name with no VPDN enabled. The redundant access to RADIUS was for DBS. This is harmless except that it slowed down session setup and put an unneeded burden on the RADIUS server. This problem has been fixed.

**CSCeb38697**

Disabling auto-negotiation on the half-height GigE card was not allowed when using release 12.2(15)BX or greater. It is now allowed.

**CSCeb39292**

The Cisco 10000 series router was sometimes unable to synchronize the configuration between the active and standby PRE. This problem was fixed.

**CSCeb44012**

The router was slow to boot when it had an ATM VBR oversubscription. This problem was fixed.

**CSCeb44881**

When you ran L2TP-related tests on the Cisco 10000 series router using Adtech AX4000 automation scripts, the following traceback messages might appear in the log:

```
*Jun 19 18:28:23.103: %GENERAL-3-EREVENT: Invalid entry Cached -Traceback= 60BF56F4
60BF6174 60AC88F8 60A6F5C4 60A8E894 60A929FC 60A8CC54 60A8D590
```

This problem was fixed.

**CSCeb48599**

When the client used PPPoE, PPPoE accounting did not work properly for PPP termination and L2TP forwarding. The Cisco 10000 series router accounted for more packets than were actually sent or received. This problem was fixed.

**CSCeb48653**

A cosmetic defect was fixed.

**CSCeb50036**

The first time PPPoX sessions with an ACL applied by a virtual template arrived at the Cisco 10000 series router, the router applied the ACL to the sessions and established the sessions as expected. However, after the PRE failed over to the redundant PRE or after a session disconnected and then reconnected with a large number of sessions, the Cisco 10000 series router attempted to apply the ACL before the session was established, which caused the following error message to appear:

```
c10k_mc_10008(config-if)#
03:29:35: %GENERAL-3-EREVENT: ACL not added to interface.
-Traceback= 60BC8FA4 6052E378 603373C0 60348204 603483AC 607B4AD8 607B4018 607B4418
```

After the Cisco 10000 series router established the sessions, the router applied the ACL as expected and the ACL was in effect.

This problem was fixed.

**CSCeb50370**

AVP/VC hierarchic shaping feature commit problem was fixed.

**CSCeb50931**

A router configured for PPPoE could leak process memory during the PPPoE Discovery process. This problem was fixed.

**CSCeb51522**

When you used the **show diag** command on an OC-48 line card, the port information could be incorrect. This problem was fixed.

**CSCeb51644**

The **diagnostic load** command had a missing call, which could trigger a traceback message because the driver was not notified that the card was down. This problem was fixed.

**CSCeb52236**

When using the 8-port DS3/E3 ATM line card, PVCs discovered by ILMI could occasionally experience lower than expected throughput performance. This problem no longer exists in this release (it is not reproducible).

**CSCeb52520**

Symbolic links for online diagnostics incorrectly used absolute instead of relative paths. In addition, there was a SYSROOT issue, which caused build problems. These problems were fixed.

**CSCeb53380**

The benchmarked call setup rate was lower than in the previous release. This problem has been fixed.

**CSCin53678**

When an SSG uplink interface was configured with a backup interface and the primary interface failed, downstream traffic from the service to the host was not accounted properly. Upstream traffic to the service could also be dropped by SSG. The traffic might not be forwarded properly after switchover. This problem was fixed.

**CSCeb54643**

The Field Diagnostics test suite for the 1-Port Channelized OC-12/STM-4 and 4-Port Channelized STM-1/OC-3 line cards could report false test failures if the Field Diagnostics image was loaded by issuing the command **diagnostic load slot slot# fd-image-url autostart**. This problem was fixed.

**CSCeb56609**

When Class-Based Weighted Fair Queueing (CBWFQ) was configured on an interface, the line could not be fully utilized. Packets started to drop from the queue before the line was fully utilized. This problem was fixed.

**CSCeb56976**

Several Synchronous Digital Hierarchy (SDH) alarms and statistics were not working correctly for SDH channelizations when using 1-channel OC-12 or 4-channel STM-1 line cards on Cisco 10000 series routers. These alarms and statistics were as follows:

- NEWPTR counter displayed by the **show controller sonet** command did not increment.
- Alarm Indication Signal (AIS) was being asserted rather than loss of multiframe (LOMF) as displayed by the **show controller au-4-tug-3** command.
- BIP-2(TU-BIP) and FEBE counters were not incremented or stored by the **show controller au-4-tug-3** command.
- AIS was asserted under conditions where Loss of Pointer (LOP) or Payload Label Mismatch (PLM) should have been.

These problems were fixed.

**CSCeb57429**

A Cisco router could reload during the bootup process because of insufficient memory. When this situation occurred, the router generated messages similar to the following:

```
current memory block, bp = 0x63903D80,
  memory pool type is Processor
data check, ptr = 0x63903DA8
bp->next(0x605C57C0) not in any mempool
previous memory block, bp = 0x200039E1,
  memory pool type is Processor
data check, ptr = 0x20003A09
%SYS-3-BADMAGIC: Corrupt block at 63903D80 (magic 61DEC941)
```

This problem could occur on a Cisco router when

- the network configuration contained ATM PVC configurations,
- the router was configured to retrieve its configuration from a TFTP server, and
- the first attempt to make such a retrieval failed.

This problem was fixed.

**CSCeb58352**

Queues were not getting properly set up. This problem is fixed.

**CSCeb58614**

When set up as an L2TP Access Concentrator (LAC), the Cisco 10000 series router failed to fragment when the Don't Fragment (DF) bit was set to 1. This problem was fixed.

**CSCeb59041**

If you booted a Cisco 10000 series router and the startup-config had the command **no pxf queuing**, the shaping did not work correctly. This problem has been fixed.

**CSCeb59590**

Issuing a **show vpdn** command caused a high CPU load. This problem has been fixed.

**CSCeb59596**

When you reset certain Ethernet interfaces with the **hw-module** command, keepalive messages were sent over the modules while they were in a down state. This problem has been fixed.

**CSCeb59615**

Interface statistics were not working for hierarchical policy. This problem has been fixed.

**CSCeb59636**

Weighted Random Early Detection (WRED) seemed to not work on hierarchical service-policy. The router code redirected the Modular QoS CLI (MQC) in this case and failed to handle the nested policy case. These changes detect the occasions when WRED information is missing from the policy passed into the configuration function and gets the configuration information from the child policy. This problem has been fixed.

**CSCeb61516**

For a router configured with a large number of subinterfaces (such as 32,000) and PPPoEoA sessions (such as 16,000), when you issued the **clear pppoe all** command, high CPU utilization (such as 99%) was observed. This problem has been fixed.

**CSCeb61517**

vrf\_nexthop\_address() did not scale. This problem has been fixed, as a performance enhancement.

**CSCeb61694**

A primary PRE could reload because of memory corruption. This symptom was observed on a Cisco 10000 series router that was configured with redundant PREs when you entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface of a 1-port Gigabit Ethernet line card. This problem has been fixed.

**CSCeb63851**

You could not generate a correct list of subsystem information for a Cisco 10000 series router. This problem has been fixed.

**CSCeb64554**

Half-height GE line cards sometimes did not forward traffic after a router reboot. This problem has been fixed.

**CSCeb64745**

There was a missing RIP update when executing the **show run** command. When executing a **show run** command with a large configuration, a Label Distribution Protocol (LDP) state change occurred on an interface and RIP stopped processing updates on all interfaces. This problem has been fixed.

**CSCeb64770**

After router reboot, system Accounting-On packets were sometimes not sent as the first packet. This problem has been fixed.

**CSCeb65193**

With all multiplexed sessions using a Port-Type of virtual and the same port value, the distinction between different session types was no longer possible. This problem was encountered by customers that have a mix of PPPoX and IP over RBE/ATM sessions emanating from the same edge device and were relying on the two sessions sending a different VSA. This problem has been fixed.

**CSCeb65477**

Executing the command **show aaa user all** could result in a router crash. This problem has been fixed.

**CSCeb66549**

A Cisco 10008 router running Cisco IOS Release 12.2(16)BX or greater could crash when a **show tech-support** or **show hardware pxf cpu statistics** command was issued. This happened if a user terminated a PPP connection with per-user access-list applied while the **show** command was being run. This problem was fixed.

**CSCeb66887**

For PPPoE sessions that had Session-Timeout, Idle-Timeout, and Ascend-Max-Time applied through RADIUS, Subscriber Service Switch (SSS) could leak memory. This problem has been fixed.

**CSCeb66894**

The router did not forward traffic from a user (client) to the service (service network), if the destination address of the service fell in the network 0.0.0.0 (the whole internet) with a non-zero subnet mask; for example, the network address was any IP address belonging to the network 0.0.0.0 and the subnet-mask was 128.0.0.0. This problem has been fixed.

**CSCeb66956**

It was thought that the input policing on a POS interface was not accurate using some IP packet sizes. However, there was a miscalculation. When input policing, the policed packet is IP packet + layer 2 protocol.

**CSCeb68152**

There was a memory leak of access\_ie handles when using PPP. This problem has been fixed.

**CSCeb68158**

Large numbers of PPPoE sessions could use all available I/O memory. This problem has been fixed.

**CSCeb68581**

Temperature alarm thresholds were raised to compensate for a problem in the PRE2 temperature sensor. This problem could trigger an alarm when the room temperature was adequate.

**CSCeb73151**

For a Cisco 10000 (ESR) series router, when configuring a VP tunnel on an ATM interface, the first created VP tunnel would go into an inactive state. The second VP tunnel could be configured without any problem. This problem was fixed.

**CSCeb73205**

Previously, you were not able to configure the AVP 38 value (the RX connect speed, remote to LAC direction) at the LAC so that it could be different from the TX connect speed or the downstream speed. An **rx-speed** command was added to support this functionality.

**CSCeb73758**

When you changed the encapsulation of a LAN subinterface to dot1q encapsulation while the subinterface was shut down, traceback messages could appear, the VLAN might not be enabled, and the output of the **show hardware pxf cpu subblocks** privileged EXEC command listed “noSB” for the affected subinterface. This problem has been fixed.

**CSCeb73765**

The new **atm over-subscription-factor** command is not longer hidden under the service internal scheme.

**CSCeb75889**

PRE High Availability (HA) Stateful Switchover (SSO) information about the running state of the system should not be synchronized from primary to secondary. When using a per-user ACL, this information was copied over. The problem has been fixed.

**CSCeb78329**

After an RPR+ switchover occurred, the deletion of an existing PVC/permanent virtual path (PVP) failed. This situation prevented you from recreating the same PVC/PVP. You could create a new PVC/PVP, but once you deleted it, you could not recreate it because the PVC remains in the active state. This problem was fixed.

**CSCeb78831**

In a pair of redundant routers, the secondary failed to reinitialize after a **hw-module sec-cpu reset** command. This problem has been fixed.

**CSCeb81177**

PPP could cause unnecessary AAA IDs to be allocated. This symptom was observed on a Cisco router that had a lot of traffic with many sessions going up and down. Over time, this symptom could cause a memory leak that would deplete the system memory. This problem was fixed.

**CSCeb81383**

There was an error in a CLI comment. It was fixed.

**CSCeb81483**

When you erased a police configuration in a policy-map, using the command **no police CIR Bc Be**, and then reconfigured a new police with a new parameter (or the same), the classifier did not work. This problem was fixed.

**CSCeb85177**

Everytime a PPPoA session was established, the following message was incorrectly added to the log:

```
Couldn't get main subinterface's tt_if_info
```

This problem was fixed.

**CSCeb85308**

After a PXF event that resulted in a PXF crash, the PXF Crashinfo file displayed Toaster register settings that did not reflect the actual values in the Toaster registers. This was caused by a data type mismatch in which bytes were read out of word-long register locations. This problem was fixed.

**CSCeb86307**

When tunneling from a LAC to an L2TP network server (LNS) using L2TP, when the LAC was configured to authenticate the user to RADIUS before negotiating the tunnel with the LNS (using the command **authen-before-forward**), it would authenticate, but would never attempt to establish the tunnel. The user would be authenticated to the RADIUS server, but the session was never tunneled to the LNS, and eventually shut down. This problem has been fixed.

**CSCeb86699**

An Accounting-On packet was not being sent after a redundancy failover. This problem has been fixed.

**CSCec00165**

Transfer error ACK (TEA) RIP route updates could be lost under heavy load (over 10,000 sessions). This problem has been fixed.

**CSCec01733**

debug message component type = ??? was logged when debugging was not enabled. This problem has been fixed.

**CSCec01759**

After running Field Diagnostics tests on an 8-port Fast Ethernet line card, tracebacks were observed. This was due to a packet numbering problem. After running the basic test suite, if the **show diag slot-number/subslot-number EXEC** command was issued within 30 seconds of the test completion, some traceback messages were displayed because the system was not able to retrieve identification programmable read-only memory (IDPROM) information. This problem was fixed.

**CSCec01803**

When running Field Diagnostics as follows, the router could get into infinite boot LCDOS loops under the following circumstances:

1. Shut down a line card in slot *x*.
2. Unplug the line card from the slot and then plug in a different type of line card.
3. Enter the **diagnostic load slot** *slot\_number* command.

This problem has been fixed.

**CSCec01915**

When using PPPoEoA, PPPoA, PPPoE, PPPoEVlan, and scale L2TP tunnels, the aggregated call setup rate decreased. Using the same setup and the Cisco IOS Release 12.2(15)BX image, the call setup rate was better. Using the same setup and the Cisco IOS Release 12.2(16)BX image, the call setup rate decreased. This problem has been fixed.

**CSCec02793**

After running for approximately three to four days, the router started rejecting new PPPoE sessions because it was unable to create the SSG sub-block. If a user tried to establish the PPPoE session several times, they usually were successful only after 10 to 15 tries. Users already connected did not experience a problem, unless they closed their PPPoE session. This problem has been fixed.

**CSCec02911**

IP packets were dropped when there was a heavy load, such as 10,000 simultaneous sessions. This was particularly applicable to L2TP tunnel configurations, which generate a lot of IP traffic in the form of hello packets and hello acqs. This problem has been fixed.

**CSCec03047**

The following traceback could appear after a microcode reload:

```
Jul 24 01:08:32.775 BRAZIL: c10k_ttcmm_write: Illegal access to toaster memory, state=0.
Jul 24 01:08:32.775 BRAZIL: c,r=0,0, flags=0x00000000, src=0x636C6260, dst=0x73459940,
len=8
Jul 24 01:08:32.775 BRAZIL: -Traceback= 60B7966C 60BED2CC 60BED7B4 60BEC4B0 60B6918C
60B6A258 60B6AF0C 60270150 60270ABC 602674D8 602692BC 602698F0 60549BA8 60C74F8C 60C750B8
6071A990
```

This problem has been fixed.

**CSCec04043**

Under certain conditions, inserting an OC48POS line card while running traffic caused a crash. This problem has been fixed.

**CSCec04525**

PPPoE protocol packets were lost when **atm pxf queuing** was used in some configurations. This problem has been fixed.

**CSCec05917**

In some cases, illegal access to a low address was given. If you issued a **hw-m sl shut** command and then a **no hw-m sl shut** command, followed by a **no card cmd** command, a bus error exception occurred. This problem has been fixed.

**CSCec07584**

When loading software into a chassis with an OC-12 ATM line card or inserting an OC-12 ATM line card into the chassis after a reload, software reload could occur. You would receive the following error:

```
Failed to allocate flowbit free entries error.
```

This problem has been fixed.

**CSCec10475**

When multiple queuing policies were configured and one of those policies was applied to an ATM virtual circuit on a p-to-p interface, an assertion failure was reported. This problem was fixed.

**CSCec11567**

Blocks of defined PVCs, even though present in the running configuration, were deleted from the line card and were no longer functional. This problem occurred when a configuration was copied into the running configuration more than once. When the maximum quantity of interfaces was present on an interface, the subsequent application of the configuration was interpreted as improper and a block of PVCs was incorrectly deleted. This problem was fixed.

**CSCec11657**

Traffic was misdirected on Ironbus from one slot to next. This problem has been fixed.

**CSCec21999**

Sometimes when reloading the router, a port on the card might display a liquid crystal display (LCD) alarm. This alarm would bring the controller and interface down. The router was unable to pass traffic because of the down interface. This problem has been fixed.

**CSCec22993**

On a highly scaled Cisco 10000 series Internet router, when the line card was reset, a Versatile Traffic Management System (VTMS) Link Unavailable error appeared. This problem has been fixed.

**CSCec23272**

When creating multipoint variable bit rate (VBR) VCs in PXF queuing mode, queues and a VTMS link are assigned to each of the PVCs. These queues were not deleted when the VBR VCs were destroyed. This problem was most evident on a highly scaled chassis with large numbers of multipoint VBR VCs: when reset, queue allocation errors appeared. For example:

```
Cannot create default queues.
```

```
Cannot allocate a new VTMS link  
Link ID exhausted.
```

This problem was fixed.

**CSCec23827**

RADIUS authentication and authorization did not operate properly after a PRE2 failover. This problem has been fixed.

**CSCec24846**

Gigabit Ethernet did not become available until approximately one minute after the system was ready following a reboot. This meant that a system accounting packet would not go out as the first record if sessions were establishing while the system was coming up. This problem was fixed.

**CSCec28894**

The **show run** command would hang the console if the configuration referenced a non-existent policy. This problem has been fixed.

**CSCec29470**

A router used as a PPPoEoA aggregator could start dropping the outgoing control plane packets, such as PPPoE discovery, PPP keepalives, and so on. This was service-disrupting. This problem was fixed.

**CSCec35717**

There could be a bus error when a user session expired due to a RADIUS Idle-Timeout (attribute 28). This problem has been fixed.

**CSCin19155**

When the exponential backoff feature is configured using the command **radius-server backoff exponential max-delay max-delay backoff-retry retry-count**, the delay (timeout) between the two retransmitted requests in the exponential backoff mode should double until it reaches the max-delay value and then it should stabilize at max-delay. The timeout was doubled for each retry but it did not stabilize at max-delay. This problem was fixed.

**CSCin24660**

The system could crash if a switchover was requested before the secondary boot completed. Specifically, on a router in SSO mode with hot standby, do a secondary reload using the **hw-module standby-cpu reset** command. Wait for the secondary to boot. After the secondary is about to complete booting, issue the switchover with a **redundancy force-switchover main-cpu** command from the active router. Keep issuing this command until the active router accepts the command.

This problem was fixed.

**CSCin42216**

If tunnel accounting was enabled and an L2X tunnel was initiated, spurious memory access could be observed at the router. This problem has been fixed.

**CSCin52591**

Previously, SSG did not restrict RADIUS packets accepted for SSG control processing. This problem has been fixed.

SSG accepts RADIUS requests from SESM for various session control functions like account logon/logoff and service logon/logoff. Previously, SSG would process any RADIUS packets received on the port on which it was listening for requests from SESM. There was no configuration option to specify which SESMs can control the SSG. The validation of the message authenticator prevented SSG from processing requests from illegal clients. But this involves computing the authenticator as well as looking for VSAs in the RADIUS requests. This processing can be avoided for RADIUS packets received from invalid clients if there was a configuration option to list the valid SESMs on SSG. SSG would only process RADIUS requests that pass the ACL configured. The configuration option on SSG is now:

```
[no] ssg radius-helper filter { acl-name | acl-number }
```

## Resolved Caveats in Cisco IOS Release 12.2(16)BX

This section describes caveats that were fixed in Cisco IOS Release 12.2(16)BX.

### CSCea51673

If you enter the **show ip dhcp pool** command, and if the output to the console is paused (requiring that you press any key to view the second page of that output), the statistics might be incorrect. This has been fixed.

### CSCea52771

When a PPPoE over Ethernet sessions is connected to the Cisco 10000 series router and the RADIUS NAS-Port format is **format a**, NAS-Port[5] is set as Virtual (60000 plus the interface number) in SSG. This has been fixed.

### CSCea78489

(Duplicate of CSCea34862) When an AAA server group is defined in the startup configuration file, the eboot image c10k2-eboot-mz displays the following message on the console:

```
% Image does not support any AAA protocols.  
% Image does not support any AAA protocols.
```

The eboot image does not need to support AAA because the eboot image does not initialize the AAA routines. The AAA commands in the startup configuration cause this message to appear during system startup. Ignore the message. Cisco IOS Release 12.2(16)BX supports AAA and it is available when the router is initialized.

### CSCea78899

If you have an OC-48 line card installed in the Cisco 10000 series router that is transmitting and receiving traffic, and you remove it and install a channelized CT3 line card, and you then remove the channelized CT3 line card and re-insert the OC-48 line card, the POS interface flaps continuously.

The OIR feature for the Cisco 10000 series router does not retain configurations when you insert a different type of line card in the same slot. This is expected behavior.

### CSCeb01423

A memory leak might occur on the Cisco 10000 series router during the installation of per user ACLs that are downloaded from a RADIUS server. This has been fixed.

### CSCeb02966

(Duplicate of CSCea40788) When you use the range command to create an oversubscription of VCs in a VP, the Cisco 10000 series router cannot create the VCs due to the oversubscription, and returns an error. The router then stops responding. This has been fixed.

### CSCeb02896

SSG fails after a PPP client attempts to log out. This problem happens when an ACL is configured with a PPP user host key. This has been fixed.

### CSCeb05601

Users cannot log back in after the primary PRE switches-over to the redundant PRE. This has been fixed.

**CSCeb12470**

When numerous per-user ACLs are configured on the router, the following error and traceback messages might display if the router is busy deleting the unused ACLs of disconnected sessions.

```
May  9 18:24:26.286: %SYS-3-CPUHOG: Task ran for 2692 msec (64/1),
process = TurboACL, PC = 60B99A88.
-Traceback= 60B99A90 602AB000 602AB27C 602ADF20 602AE0B4 602AE3B4
```

This has been fixed.

**CSCeb13130**

When a Path Link Mismatch (PLM) alarm exists on the 1-port channelized OC-12 line card or the 4-port channelized OC-3 line card, the **show controller** command for T1 or E1 controller that is configured for SDH framing does not display the PLM alarm. The alarm does display correctly if SONET framing is configured. This has been fixed.

**CSCeb24714**

The Cisco 10000 series router takes longer than expected (approximately 90 minutes) to load the 16M configuration file. The elog file indicated that the fib-get-auto-adjacency\_fibidb function was sampled at a large percentage (approximately 11%). This has been fixed.

**CSCeb24732**

The Cisco 10000 series router takes longer than expected to load the router configuration. If you enter the **show parser stat** command while the router is loading the configuration, a lot of cache misses display. This has been fixed.

**CSCeb24738**

The Cisco 10000 series router is slow to boot when you add the static route improvement patch code. This has been fixed.

**CSCeb24747**

The Cisco 10000 series router is slow to load while you set up subinterfaces. This has been fixed.

**CSCeb26584**

After the absolute timeout expires for PPPoE sessions with per user ACLs, the router disconnects the sessions. If you then enter the **show pxf cpu access-list security** command, numerous “Unneeded ACLs” display. This has been fixed.

**CSCeb29038**

A bus error occurs when executing the **show pxf cpu access-lists security** command after sessions time out and start to disconnect. This has been fixed.

**CSCeb29043**

A memory leak might occur in the process AAA Per-User when PPPoE sessions are brought up, then torn down, then brought up again. This has been fixed.

**CSCeb29165**

You cannot ping the default network when the **ip verify unicast reverse-path** command is configured under the Virtual Template. You can only ping the default network when you are logged in to the service. This has been fixed. The routes to a downlink interface and SSG hosts are now added to the service VRF tables, which allows RPF checks for SSG hosts that have not yet logged on to any services.

This does not work with static routes added for RPF checks. Only interface network addresses are added to the SSG VRFs. Static routes for hosts are not added to the SSG VRFs and RPF checks might fail. This can occur if you configure the **ip unnumbered** command on downlink interfaces with static routes.

SSG adds the route when binding the interface. If you change the interface address after the interface is bound, SSG cannot track the interface.

**CSCeb29285**

When a user logs out of a session with accounting, the NAS ID is incorrect. This problem occurs with the Accounting Stop packet in a PPPoE configuration. This has been fixed.

**CSCeb31501**

The Cisco 10000 series router does not send out a TERMREQ when the router clears a PPPoA virtual access interface. This has been fixed.

**CSCeb31520**

The Cisco 10000 series router stops responding when you enter the **clear interface virtual-access number** command for a PPPoA VAI with a conditional **debug** interface turned on. This has been fixed.

**CSCeb31714**

On an ATM interface with UBR traffic shaping configured, the router shapes the traffic incorrectly. This does not occur when you set high thresholds. Be careful not to set the thresholds so high that with typical traffic patterns, the SAR buffer becomes full.

**CSCeb33336**

The session connection rate appears to be unacceptably slow when SSG accounting is enabled. This has been fixed.

The connection rate for sessions with SSG accounting enabled are typically 3 to 4 percent higher than the connection rate for sessions with SSG accounting disabled. This is due to the time required for the SSG router to receive the accounting information from RADIUS.

**CSCeb38319**

The line cards go down and remain down after the Cisco 10000 series router reloads or a forced failover to the redundant PRE is executed. This has been fixed.

**CSCeb39442**

The Cisco 10000 series router does not update the QoS shaping parameters for a VC when DBS is enabled on a VC class.

If you enter the **show atm pvc dbs** command when a PPPoA session is established, the output from the command indicates that RADIUS is sending the AV pairs, but the shaping parameters for the VC are unchanged. The Cisco 10000 series router does not change the VC and instead displays an error message similar to the following:

```
Jun  5 13:21:19.200: %C10K DBS: validate_params() 2/111, vcd 11,
QoS type 5, PCR 50, SCR 38
Jun  5 13:21:19.200: %C10K DBS: validate() QoS update rejected
PVC 2/111 on VP tunnel
```

This has been fixed.

**CSCeb39820**

The Cisco 10000 series router might stop responding while processing turbo ACLs. This has been fixed.

**CSCec28894**

The **show run** command would hang the console if the configuration referenced a non-existent policy. This problem has been fixed.

**CSCec29470**

A router used as a PPPoEoA aggregator could start dropping the outgoing control plane packets, such as PPPoE discovery, PPP keepalives, and so on. This was service-disrupting. This problem was fixed.

**CSCec35717**

There could be a bus error when a user session expired due to a RADIUS Idle-Timeout (attribute 28). This problem has been fixed.

## Other Caveats

This section includes caveats listed in previous release notes that are regarded as resolved because they are either unreproducible, they were reported in error, or they do not affect the behavior of the Cisco 10000 series router. If a caveat listed in this section causes problems, contact Cisco customer service.

**CSCdy64397**

The LNS sends keepalives at an incorrect interval. We have been unable to reproduce this problem.

**CSCea33889**

Previously, it was reported that the output of the **show controller e1** command showed the status of the E1 controller on the 24-port channelized E1/T1 line card as down when it was actually up. We have been unable to reproduce this problem.

**CSCea78453**

In rare circumstances, if you enter the **hw-module slot slot shutdown** command followed by the **no card** command, the router reloads unexpectedly. This problem rarely occurs and you are unlikely to experience it. We have been unable to reproduce this problem.

# Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn. Document Resource Connection  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

### Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

### Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

## Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

<http://www.cisco.com/go/packet>

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0304R)

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

