



# Release Notes for the Cisco 10000 Series Router for Cisco IOS Release 12.2(16)BX2

---

**January 5, 2004**

Cisco IOS Release 12.2(16)BX2

OL-4065-04

These release notes for the Cisco 10000 series router support Cisco IOS Release 12.2(16)BX2, which provides Service Selection Gateway features for the Cisco 10000 series 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 recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at [http://www.cisco.com/warp/customer/tech\\_tips/index/fn.html](http://www.cisco.com/warp/customer/tech_tips/index/fn.html). If you do not have a Cisco.com login account, you can find field notices at [http://www.cisco.com/warp/public/tech\\_tips/index/fn.html](http://www.cisco.com/warp/public/tech_tips/index/fn.html).

## Contents

This document contains the following sections:

- [Inheritance Information, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 2](#)
- [Limitations and Restrictions, page 4](#)
- [Important Notes, page 6](#)
- [Caveats for Cisco IOS Release 12.2\(16\)BX2, page 11](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation, page 20](#)
- [Documentation Feedback, page 21](#)
- [Obtaining Technical Assistance, page 21](#)
- [Obtaining Additional Publications and Information, page 22](#)



---

**Corporate Headquarters:**

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

# Inheritance Information

Cisco IOS Release 12.2(16)BX2 is based on the following releases:

- Cisco IOS Release 12.2(16)BX1
- 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>

## System Requirements

Cisco IOS Release 12.2(16)BX2 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 general information about upgrading to a new software release, refer to *Software Installation and Upgrade Procedures* located at the following URL:

[http://www.cisco.com/en/US/products/hw/routers/ps133/products\\_tech\\_note09186a0080094c07.shtml](http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080094c07.shtml)

## New and Changed Information

The following section lists the new software features supported by the Cisco 10000 series router for Cisco IOS Release 12.2(16)BX2:

- [New Features—Cisco IOS Release 12.2\(16\)BX2, page 3](#)

For information about new features supported on the Cisco 10000 router in other releases, see the appropriate release notes at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10krn/index.htm>

## New Features—Cisco IOS Release 12.2(16)BX2

The following new feature and enhancements are supported on the Cisco 10000 router in Cisco IOS Release 12.2(16)BX2:

- [Half-Duplex VRF](#), page 3
- [SSG Enhancements for Overlapping Service Definitions](#), page 3

### Half-Duplex VRF

The Half-Duplex VRF (HDVRF) feature provides scalable hub and spoke connectivity for subscribers of a multiprotocol label switching-based virtual private network (MPLS VPN) service. These subscribers connect to the provider edge (PE) router of the wholesale service provider, and they use the same or different services (for example, the same or different VRFs). The HDVRF feature prevents local connectivity between subscribers at the spoke PE router and ensures that a hub site provides subscriber connectivity. Any sites that connect to the same PE router must forward intersite traffic using the hub site. This ensures that the routing done at the spoke site is always access side interface to network side interface, or network side interface to access side interface, and never access side to access side.

For more information, see the *Half-Duplex VRF* feature module, located at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10kfm/index.htm>

### SSG Enhancements for Overlapping Service Definitions

Overlapping services are services for which the route prefix of one service matches or is contained within the route prefix of another service. For example, the service definition 172.16.253.0/24 overlaps with the service definition 172.16.0.0/16 because the prefix 172.16 is contained in both definitions. The definition 0.0.0.0/0 overlaps all other possible services.

In releases prior to Cisco IOS Release 12.2(16)BX2, the Cisco 10000 router does not allow users to be subscribed to a service if that service overlaps another service to which a different user is subscribed.

To enable service providers to use existing overlapping definitions, the Cisco 10000 router provides the following SSG enhancements:

- **Service Translation**—Translates overlapping service definitions to a set of non-overlapping service definitions.
- **Expansion of Service IDs**—Expands the number of service IDs supported from seven to 15. The router uses service IDs to determine which services a user is subscribed to and how to police the user traffic.

To enable service translation on the router, enter the **ssg service-overlap** command in global configuration mode. This command indicates to the router to use the translated network sets to provide the desired network behavior.

For more information, see the “SSG Enhancements for Overlapping Services” section in the “Miscellaneous SSG Features and Enhancements” chapter of the *Cisco 10000 Series Router Service Selection Gateway Configuration Guide*.

## 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 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** 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 authentication, authorization, and accounting (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 releases supports a maximum of 8000 unshaped unspecified bit rate permanent virtual circuits (UBR VCs) on the OC-12 ATM line card. An unshaped UBR PVC is a PVC that has no rate configured on it. You can configure up to 16,000 shaped UBR PVCs per port on the OC-12 line card if you configure the PVCs with a shaped rate of less than 299 Mbps.

## Shaped UBR PVCs

The Cisco 10000 series router does not support shaped UBR in atm pxf queuing 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)BX2:

- [Interoperability with Test Equipment, page 7](#)
- [Provisioning for Scaling, page 7](#)
- [Enhancing Scalability of Per-User Configurations, page 9](#)
- [Inserting a New Line Card, page 11](#)

## Interoperability with Test Equipment

### CSCea57201, CSCed28815

Interoperability issues exist when using the Spirent Adtech AX/4000 with ATM connections. These conditions will not occur in a live network deployment, and only affect lab testing.

The Adtech appears to interpret packet padding, instead of ignoring it (reference ITU-T I.363.5 08/96).

Keepalive packets for PPPoA sessions are often dropped, causing sessions to drop. This behavior occurs especially when the Cisco 10000 has PPPoA and PPPoEoA on the same ATM line card, with three or more virtual path identifiers (VPIs) configured. The content of the padding in this configuration causes the Adtech to ignore the PPPoA keepalives.

More broad incompatibilities were resolved in Adtech version 4.51. This current interoperability is a more specific configuration.

## Provisioning for Scaling

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

- [CISCO-ATM-PVCTRAP-EXTN-MIB, page 8](#)
- [PPPoA Sessions with IP QoS Static Routes, page 8](#)
- [AAA Authentication on the NME Port, page 9](#)
- [Call Admission Control, page 9](#)

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*.

## CISCO-ATM-PVCTRAP-EXTN-MIB

The Cisco 10000 router does not support the CISCO-ATM-PVCTRAP-EXTN-MIB for large numbers of permanent virtual circuits (for example, 32,000 PVCs). To exclude the Cisco-ATM-PVCTRAP-EXTN-MIB from the Simple Network Management Protocol (SNMP) view and enhance scalability, configure the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>snmp-server view</b> <i>view-name oid-tree included</i>	Creates or updates a view entry.  The <i>view-name</i> argument is a label for the view record that you are updating or creating. The name is used to reference the record.  The <i>oid-tree</i> argument is the object identifier of the ASN.1 subtree to be included from the view. Specify a valid oid-tree from where you want to poll the information.  The <b>included</b> argument configures the OID (and subtree OIDs) specified in the <i>oid-tree</i> argument to be included in the SNMP view.
Step 2	Router(config)# <b>snmp-server view</b> <i>view-name ciscoAtmPvcTrapExtnMIB excluded</i>	Configures the CISCO-ATM-PVCTRAP-EXTN-MIB OID (and subtree OIDs) to be explicitly excluded from the SNMP view. You must specify the oid-tree as shown in the command line.  The <i>view-name</i> argument must match the <i>view-name</i> you specified in step 1.
Step 3	Router(config)# <b>snmp-server community</b> <i>string [view view-name] [ro   rw]</i> <i>[access-list-number]</i>	Sets up the community access string to permit access to SNMP.  The <i>string</i> argument is a community string that acts like a password and permits access to the SNMP protocol.  The <i>view-name</i> argument must match the <i>view-name</i> you specified in step 1.

[Example 1](#) shows how to create or modify the SNMP view named myview to include the information polled from the Internet oid-tree and to exclude the CISCO-ATM-PVCTRAP-EXTN-MIB oid-tree. The community access string named private is set up and access to SNMP is read-only (ro) access.

### Example 1 Excluding CISCO-ATM-PVCTRAP-EXTN-MIB from the SNMP View

```
Router(config)# snmp-server view myview internet included
Router(config)# snmp-server view myview ciscoAtmPvcTrapExtnMIB excluded
Router(config)# snmp-server community private view myview ro
```

For more information about the **snmp-server view** and **snmp-server community** commands, see the [Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3](#).

## PPPoA Sessions with IP QoS Static Routes

To scale to 32,000 PPP over ATM (PPPoA) sessions with IP quality of service (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 2](#) shows how to redefine the VRF named newyork using the ip:vrf-id VSA.

### **Example 2**     *Redefining VRF Configurations*

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

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

[Example 3](#) shows how to redefine the Loopback 0 interface using the ip:ip-unnumbered VSA.

### **Example 3**     *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.

## Caveats for Cisco IOS Release 12.2(16)BX2

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

For information on caveats in Cisco IOS Release 12.2(16)BX2, see the following sections:

- [Open Caveats—Cisco IOS Release 12.2\(16\)BX2, page 11](#)
- [Resolved Caveats—Cisco IOS Release 12.2\(16\)BX2, page 15](#)
- [Other Caveats, page 19](#)

## Open Caveats—Cisco IOS Release 12.2(16)BX2

[Table 1](#) describes open caveats in Cisco IOS Release 12.2(16)BX2.

For information about open caveats in other Cisco IOS releases, see the appropriate release notes document at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10krn/index.htm>

**Table 1** Open Caveats in Cisco IOS Release 12.2(16)BX2

Caveat	Description
<b>CSCdy79740</b>	<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> There is no workaround for this problem.</p>
<b>CSCea35508</b>	<p>The throughput of Frame Relay traffic might be up to 5 percent lower than the maximum possible throughput.</p> <p><b>Workaround:</b> There is no workaround for this problem.</p>
<b>CSCea37019</b>	<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> There is no workaround for this problem.</p>

Table 1 Open Caveats in Cisco IOS Release 12.2(16)BX2 (continued)

Caveat	Description
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 automatic protection switching (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>
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> There is no workaround for this problem.</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> There is no workaround for this problem.</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> There is no workaround for this problem.</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 data-bbox="553 1688 732 1709">%ALIGN-3-TRACE</pre> <p><b>Workaround:</b> There is no workaround for this problem.</p>

**Table 1** Open Caveats in Cisco IOS Release 12.2(16)BX2 (continued)

Caveat	Description
<b>CSCea70951</b>	<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> There is no workaround for this problem.</p>
<b>CSCea72016</b>	<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>
<b>CSCea73477</b>	<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>
<b>CSCea78861</b>	<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>
<b>CSCea81015</b>	<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>
<b>CSCeb01499</b>	<p>The following traceback message displays in the log after you enter the <b>hardware subslot shutdown, no card, and 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> There is no workaround for this problem.</p>
<b>CSCeb26165</b>	<p>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.</p> <p><b>Workaround:</b> There is no workaround for this problem.</p>

**Table 1** Open Caveats in Cisco IOS Release 12.2(16)BX2 (continued)

Caveat	Description
<b>CSCeb33056</b>	<p>The Cisco 10000 series router frequently displays the following interprocess communications (IPC) queue full message:</p> <pre>00:15:49: %IPCGRP-6-NBLKCMD_Q_FULL: Nonblocking IPC command queue full (60 commands) &lt;---</pre> <p><b>Workaround:</b> There is no workaround for this problem.</p>
<b>CSCeb35104</b>	<p>Configurations with a very large number of subinterfaces (for example, 32,000) might experience slow PPP over Ethernet over ATM (PPPoEoA) session clearing.</p> <p><b>Workaround:</b> There is no workaround for this problem.</p>
<b>CSCeb36330</b>	<p>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:</p> <pre>Jun 11 09:09:33.215: %ATM-5-UPDOWN: Interface ATM3/0/0.100, Changing autovc 3/101 to ADMIN_DOWN</pre> <p><b>Workaround:</b> There is no workaround for this problem.</p>
<b>CSCeb51344</b>	<p>RADIUS configurations that use lcp: 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> There is no workaround for this problem.</p>
<b>CSCeb53208</b>	<p>The Cisco 10000 router creates PPP sessions without allocating a virtual circuit connection identifier (VCCI).</p> <p><b>Workaround:</b> There is no workaround for this problem.</p>
<b>CSCeb53474</b>	<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> There is no workaround for this problem.</p>
<b>CSCeb77168</b>	<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>

**Table 1** Open Caveats in Cisco IOS Release 12.2(16)BX2 (continued)

Caveat	Description
<b>CSCeb77178</b>	<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>
<b>CSCec23078</b>	<p>The parallel express forwarding (PXF) engine might fail due to invalid commands being issued to the PXF. This occurs when an L2TP Network Server (LNS) receives a large IP packet from the IP cloud, the destination IP address is a PPP session to a DSL customer, and netflow is enabled on the ingress interface. The size of the packet received from the trunk and going into the L2TP tunnel must exceed the tunnel minimum transmission unit (MTU) so that fragmentation occurs.</p> <p><b>Workaround:</b> Disable netflow on the LNS.</p>
<b>CSCec24597</b>	<p>When configuring a constant bit rate permanent virtual circuit (CBR PVC) using a test script, a traceback message appeared and the router did not create the CBR PVC.</p> <p><b>Workaround:</b> There is no workaround for this problem.</p>
<b>CSCec61602</b>	<p>A memory leak occurs when a large number of SSG users are logged in and SSG accounting is enabled. Using the <b>show memory summary</b> command, the number of free bytes for processor and I/O memory diminishes rapidly and with 32,000 sessions, the memory can diminish to zero after approximately 24 hours.</p> <p><b>Workaround:</b> Disable SSG accounting.</p>
<b>CSCin46447</b>	<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> There is no workaround for this problem.</p>

## Resolved Caveats—Cisco IOS Release 12.2(16)BX2

This section describes caveats that were fixed in Cisco IOS Release 12.2(16)BX2.

For information about caveats fixed in other Cisco IOS releases, see the appropriate release notes document at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10krn/index.htm>

### **CSCea77321**

If the primary PRE failed, and the primary PRE switched over to the secondary (redundant) PRE, ODAP subnets that had been allocated to the previously active primary PRE remained marked as Leased by the Access Registrar (AR). This has been fixed.

**CSCea78890**

If you performed a **ftfp copy** of a running configuration greater than 5 MB to a trivial file transfer protocol (TFTP) server, the copy failed. This has been fixed.

**CSCea82309**

If you opened two configuration sessions on the PRE (Part Number ESR-PRE2) from two console devices, a failure message appeared on the console devices stating that simultaneous configuration was not supported. This has been fixed.

**CSCeb08194**

When SSG traffic was redirected because users were not authorized for services, CPU usage was high and throughput was limited. This is expected behavior for the amount of traffic stress on the route processor (RP).

**CSCeb17086**

Traceback messages appeared while configuring static multicast routes. This has been fixed.

**CSCeb38277**

When an ATM interface was configured as unnumbered, the Cisco 10000 series router did not forward routed bridge encapsulation (RBE) traffic to RBE clients because the router configuration was incorrect.

The Cisco 10000 router supports the Dynamic Host Configuration Protocol (DHCP) relay agent information option (Option 82) feature when ATM RBE is used to configure DSL access. The DHCP server must be configured on the router. The **ip helper-address** command must be configured on the ATM interface and the **dhcp relay** command must be configured to communicate with the DHCP server. The loopback interface is part of the VRF.

**CSCeb41285**

(Duplicate of CSCea34048) The Cisco 10000 series router did not create the virtual access interface (VAI) if the RADIUS user profile included Frame-Compression attribute-value pair (AVP). If the AVP for compression was removed from the user profile, the router created the VAI. This has been fixed.

**CSCeb48677**

Nested policies configured on the main interface of the Gigabit Ethernet (GE) line card did not work. Nested policies configured on GE subinterfaces did work properly.

Nested policies are intended to be used only on subinterfaces and not on main interfaces. A nested policy is not necessary to shape off the main interface. Nested policies are functional only on subinterfaces such as IEEE 802.1Q VLAN GE subinterfaces and ATM VCs.

**CSCeb52243**

On the 8-port DS3/E3 ATM line card, F5 Operation, Administration, and Maintenance (OAM) Rate Limiting did not properly drop the OAM cells that exceeded the rate limit.

The Cisco 10000 router does not support the OAM Rate Limiting feature for Cisco IOS Release 12.2(16)BX.

**CSCeb53344**

During sweep ping testing of the 8-port DS3/E3 line card, a single ping failure occurred. This has been fixed.

**CSCeb54544**

When a VC class had an autopp encapsulation configured, if you created a new VC class by entering the **vc-class** command or you made changes to an existing VC class, the Cisco 10000 series router deleted all of the VCs that were included in the VC class with autopp encapsulation and then created the VCs again. This has been fixed.

**CSCeb54587**

When a service policy was configured in a virtual template, the following error message appeared as the session was being established:

```
Couldn't get main subinterface's tt_if_info from c10k_check_should_policy_be_applied
```

This was not an error condition. This message was an obsolete message. The service policy was applied as expected. This has been fixed.

**CSCeb55625**

When you hot swapped an 8-port DS3/E3 ATM line card with a 1-port OC-12 POS line card, the following traceback message appeared. The Cisco 10000 series router properly provisioned the 1-port OC-12 POS line card.

```
*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
```

This has been fixed.

**CSCeb58934**

After you issued a **debug qos-set** command, the debug output of the command was not disabled with the **no debug all** command and it did not appear in the output of the **show debug** command. This has been fixed.

**CSCeb59318**

When a user profile on the RADIUS server included the AV-pair Framed-Compression = None, the virtual interface was created on the router. The fix that enabled the virtual interface (CSCeb41285) caused another issue. When the router negotiated the parameters for the session with the RADIUS server, a full VAI was created if the AV-pair Framed-Compression existed in the user profile.

This is expected behavior for the Framed-Compression command. The None option is used to turn off VJ header compression and it always creates full VAIs.

**CSCec15506**

(Duplicate of CSCec71906) The PPPoEoA call setup rate with per-user ACLs did not exceed 22 calls per second (cps), which was significantly lower than the expected performance of 50 cps. This has been fixed.

**CSCec34475**

If you loaded a Field Diagnostics image from disk0, the router could fail. This has been fixed.

**CSCec48810**

When a service policy was applied to the interface, traffic was dropped in the default queue. Reloading the router fixed the problem. This has been fixed.

**CSCec48814**

When deleting an explicitly configured default queue from the service policy, the default queue was deleted in the PXF. This resulted in packets being dropped when they were sent to the default queue. If the complete service policy was then removed from the interface, the packet priority queue was the only queue present in the PXF for the interface. All traffic was dropped. This has been fixed.

**CSCec65343**

When starting up 32,000 sessions, SYS-3-CPUHOG messages for the Simple Network Management Protocol (SNMP) engine sometimes appeared. This occurred when the Cisco 10000 router was polling SNMP MIBs.

The Cisco 10000 router does not support CISCO-ATM-PVCTRAP-EXTN-MIB for a large number of PVCs (for example, 32,000 PVCs). Therefore, you must exclude the CISCOATMPVCTRAPEXTNMIB oid-tree from the SNMP view. To do this, enter the following commands in global configuration mode:

```
Router(config)# snmp-server view view-name oid-tree included
Router(config)# snmp-server view view-name ciscoAtmPvcTrapExtnMIB excluded
Router(config)# snmp-server community string [view view-name] [ro | rw]
```

For more information, see the “CISCO-ATM-PVCTRAP-EXTN-MIB” section on page 8 or the [Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3](#).

**CSCec80816**

The PXF failed when the Cisco 10000 router functioned as an L2TP Network Server (LNS). This occurred only when a packet was reassembled, multihop tunnel-switched, and then fragmented going into the other L2TP tunnel. This has been fixed.

**CSCed07736**

A software watchdog event occurred while defragmenting Dynamic ACL memory allocations. This has been fixed.

**CSCed27956**

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

## 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. See the [“Obtaining Technical Assistance” section on page 21](#).

### **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.

### **CSCeb21692**

A client was unable to ping the SSG access side downlink interface. This occurred when an SSG interface was configured as a downlink interface and routing with bridged encapsulation was configured. We have been unable to reproduce this problem.

### **CSCeb42938**

The following traceback message randomly appeared:

```
00:48:42: %AAA-3-BADMETHOD: Cannot process authorization method 1635568848
-Process= "AAA Server", ipl= 0, pid= 58
-Traceback= 603B6A1C 603AFE24 603B0C58 603B0D78
```

We have been unable to reproduce this problem.

### **CSCeb49776**

Multiple memory leaks occurred while testing the Cisco IOS Release 12.2(16)BX image. We have been unable to reproduce this problem.

### **CSCeb51308**

When 61,500 PPPoEoA sessions were active and SNMP was running in the background, executing the **show ios** command caused the following traceback message to appear:

```
05:21:32:%SYS-3-CPUHOG:Task ran for 4120 msec (464/222),
process = Virtual Exec, PC = 604F8360.
```

We have been unable to reproduce this problem.

## Related Documentation

The following documents are specific to Cisco IOS Release 12.2(16)BX2:

- [Cisco 10000 Series Router Service Selection Gateway Configuration Guide](#)
- [Cisco 10000 Series Broadband Aggregation Configuration Guide](#)
- [Cisco 10000 Series Router Feature Map](#)
- [Cisco 10000 Series Router Command Quick Reference Guide](#)

## Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

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

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Click Subscriptions & Promotional Materials in the left navigation bar.

### Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit e-mail comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

### Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

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

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

## TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## 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 general networking, training and certification titles. Both new and experienced users will benefit from these publications. 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/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/index.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 © 2004, Cisco Systems, Inc.  
All rights reserved.

