



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

---

June 17, 2004

These release notes provide information about Cisco IOS Release 12.2(16)BX, 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)BX is based on the following releases:

- 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/reInote/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 © 2003–2004 Cisco Systems, Inc. All rights reserved.

# Contents

This document contains the following sections:

- [Cisco Security Advisory, page 2](#)
- [System Requirements, page 2](#)
- [New Features—Cisco IOS Release 12.2\(16\)BX, page 3](#)
- [Software Features Supported on the Cisco 10000 Series Router, page 11](#)
- [Limitations and Restrictions, page 12](#)
- [Important Notes, page 14](#)
- [Open Caveats—Cisco IOS Release 12.2\(16\)BX, page 16](#)
- [Resolved Caveats—Cisco IOS Release 12.2\(16\)BX, page 23](#)
- [Other Caveats, page 27](#)
- [Obtaining Documentation, page 27](#)
- [Obtaining Technical Assistance, page 28](#)
- [Obtaining Additional Publications and Information, page 30](#)

## Cisco Security Advisory

Cisco routers and switches that are running Cisco IOS software and that are configured to process Internet Protocol Version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device might cause the input interface to stop processing traffic when the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices that are running only IP Version 6 (IPv6) are not affected.

Cisco has made software available, free of charge, to correct the problem. For more information, refer to the *Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packet*, located at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>

## System Requirements

Cisco IOS Release 12.2(16)BX 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)BX

The following new features and improvements are supported on the Cisco 10000 series Internet router in Cisco IOS Release 12.2(16)BX:

- [Service Selection Gateway, page 3](#)
- [Field Diagnostics, page 9](#)
- [8-Port DS3/E3 ATM Line Card, page 10](#)

The following sections describe these features.

### Service Selection Gateway

The Cisco 10000 series router supports the following Service Selection Gateway (SSG) features in Cisco IOS Release 12.2(16)BX:

#### Access Protocols

- Subscriber side—PPPoE, PPPoA, RBE, RFC 2684 IP
- Network side—ATM PVCs and subinterfaces, Ethernet interfaces and subinterfaces, POS interfaces, serial and channelized interfaces

#### SSG Logon and Logoff

- [Single Host Logon, page 4](#)
- [SSG Autologoff, page 5](#)
- [SSG Prepaid and SSG Prepaid Idle Timeout, page 5](#)
- [SSG Session and Idle Timeout, page 5](#)

#### Authentication and Accounting

- [SSG Full Username RADIUS Attribute, page 5](#)
- [Account Login and Logout, page 5](#)
- [Service Connection and Termination, page 6](#)

#### Service Selection Methods

- [PPP Terminated Aggregation, page 6](#)
- [PTA-Multidomain, page 6](#)
- [Web Service Selection, page 6](#)

**Service Connection**

- [SSG AutoDomain, page 6](#)
- [SSG Open Garden, page 7](#)
- [SSG Port-Bundle Host Key, page 7](#)
- [Exclude Networks, page 7](#)
- [Mutually Exclusive Service Selection, page 7](#)

**Service Profiles**

- [Service Profiles and Cached Service Profiles, page 7](#)

**Interface Configuration**

- [Transparent Passthrough, page 8](#)
- [Multicast Protocols on SSG Interfaces, page 8](#)

**Policing**

- [SSG Hierarchical Policing, page 7](#)

**Redirection**

- [SSG TCP Redirect, page 8](#)

**Miscellaneous Features**

- [VPI/VCI Static Binding to a Service Profile, page 8](#)
- [RADIUS Virtual Circuit Logging, page 8](#)
- [AAA Server Group Support for Proxy Services, page 9](#)
- [Packet Filtering, page 9](#)
- [SSG Unconfig, page 9](#)
- [Per-Service Statistics, page 9](#)

The following sections describe the Service Selection Gateway features. For more information on configuring these features, refer to the *Cisco 10000 Series Internet Router Service Selection Gateway Configuration Guide*.

## Single Host Logon

The Single Host Logon feature enables SESM to authenticate subscribers by using the PPP authenticated information from the SSG; a subscriber does not need to log on to the SESM. To log on to a service through the SESM web application, a subscriber enters authentication information once for the PPP session and once for the service.

For non-PPP users, when a subscriber authenticates using the SESM application, the subscriber does not have to log on again for the remainder of the non-PPP session. However, the subscriber still has to log on to services.

## SSG Autologoff

The SSG Autologoff feature enables SSG to verify connectivity with each host. SSG checks the status of the connection with each host at configured intervals. If SSG finds that a host is not reachable, SSG automatically initiates the logoff of that host. SSG has two methods of checking the connectivity of hosts: ARP ping and ICMP ping.

## SSG Prepaid and SSG Prepaid Idle Timeout

The SSG Prepaid feature allows a user to connect to a service if the user has prepaid for the service. The SSG Prepaid feature is time-based only.

When SSG Prepaid is configured, SSG checks a subscriber's available credit to determine whether to connect the subscriber to the service and how long the connection can last. The billing server administers the subscriber's credit as a series of quotas. These quotas are allotments of available credit and represent the duration of use.

The SSG Prepaid Idle Timeout feature enables SSG to return residual quotas (allotments of prepaid credit) to the billing server from services that a user is logged into but not actively using. The SSG can reauthorize a user before the user completely consumes the allocated quota. The SSG Prepaid Idle Timeout feature also enhances the handling of a returned zero quota from the billing server. A user's connection to services can be open even when the billing server returns a zero quota. The SSG can notify the billing server when a connection fails, enabling the billing server to free quota reserved for the failed connection.

## SSG Session and Idle Timeout

The Session-Timeout RADIUS attribute and the Idle-Timeout RADIUS attribute are two mechanisms used to prevent the SSG from continuing to allow traffic to pass from the IP address of a user who has disconnected from the network access server without logging out from the SSG. These attributes specify the following:

- Session-Timeout RADIUS attribute—Specifies the maximum length of time for which a host or connection object can remain continuously active.
- Idle-Timeout RADIUS attribute—Specifies the maximum length of time for which a session or connection can remain idle before it is disconnected.

## SSG Full Username RADIUS Attribute

The Full Username RADIUS attribute allows SSG to include the user's full username and domain (user@service) in the RADIUS authentication and accounting requests.

## Account Login and Logout

SSG sends a RADIUS accounting-request record to the local RADIUS server when a user logs in to or out of the SSG. The Acct-Status-Type attribute included in the accounting-request record indicates if the accounting-request marks the start of the user service or the end of the service.

When a user logs in, SSG sends an accounting-start record to RADIUS. When a user logs out, SSG sends an accounting-stop record.

## Service Connection and Termination

SSG also sends a RADIUS accounting-request record to the local RADIUS server when a user accesses or terminates a service. The Acct-Status-Type attribute included in the accounting-request record indicates whether the accounting-request marks the start of the user service or the end of the service.

When a user accesses a service, SSG sends an accounting-start record to RADIUS. When a user terminates a service, SSG sends an accounting-stop record.

## PPP Terminated Aggregation

PPP terminated aggregation (PTA) is a PPP selection method in which service selection is based on a structured domain name (for example, username@service.com). PTA terminates the PPP session into a single routing domain. Users can only access one service and users do not have access to the default network or SESM.

The PTA-MD exclusion list allows you to create a set of domains that you want to exclude from SSG processing.

## PTA-Multidomain

PTA-Multidomain (PTA-MD) is a PPP selection method in which service selection is based on a structured domain name (for example, username@service.com). PTA-MD terminates the PPP sessions into multiple IP routing domains. SSG features and processing are applied to the user traffic and users can access one or more services at a time. PTA-MD service selection supports a wholesale VPN model where each domain is isolated from the other and has the capability to support overlapping IP addresses.

## Web Service Selection

Web service selection enables users to concurrently access multiple on-demand services from a list of personalized services. The Cisco 10000 series Internet router supports the Cisco Subscriber Edge Services Manager (SESM) application for web service selection.

The SESM application provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with the SESM web application using a standard Internet browser. They do not need to download any software or plug-ins to use the SESM web pages. After a subscriber successfully authenticates, the SESM web application presents a list of services that the subscriber is currently authorized to use. The subscriber can gain access to one or more of those services by selecting them from a web page. Alternatively, an automatic connection feature might provide automatic connection to services.

## SSG AutoDomain

The SSG AutoDomain feature allows users to automatically connect to a service based on the domain part of the structured username specified in an Access-Request. When SSG AutoDomain is configured, user authentication is performed at the service (for example, at the AAA server within a corporate network), instead of at the network access server (NAS).

## SSG Open Garden

An Open Garden is a collection of networks or web sites that subscribers can access as long as they have physical access to the network. Subscribers do not have to provide authentication information before accessing the networks in an Open Garden. The network is not restricted by service selection, subscription, or policing.

## SSG Port-Bundle Host Key

The SSG Port-Bundle Host Key feature enhances communication and functionality between SSG and SESM by introducing a mechanism that uses the host source IP address and source port to identify and monitor subscribers. With the SSG Port-Bundle Host Key feature, SSG performs port-address translation (PAT) and network-address translation (NAT) on the HTTP traffic between the subscriber and the SESM server.

## Exclude Networks

The Exclude Networks feature allows you to specify networks that you do not want users to automatically log on to.

## Mutually Exclusive Service Selection

The Mutually Exclusive Service Selection feature restricts a subscriber to accessing only one service at a time in a specified group of services.

## Service Profiles and Cached Service Profiles

Service profiles define the services that subscribers can select. Each service that is accessible has a profile that defines the attributes of the service. Service profiles are configured on the RADIUS server or directly on the Cisco 10000 series Internet router. The RADIUS server or SESM downloads the service profiles to the router as needed.

The Cached Service Profiles feature enables SSG to use a cached copy of a service profile instead of downloading the profile from RADIUS every time a user logs on to the service.

## SSG Hierarchical Policing

The traffic policing feature limits the transmission rate of traffic entering or leaving a node. In SSG, traffic policing can be used to allocate bandwidth between subscribers and between services to a particular subscriber to ensure all types of services are allocated a proper amount of bandwidth. SSG uses per-user and per-service policing to ensure bandwidth is distributed properly between subscribers (per-user policing) and between services to a particular subscriber (per-session policing). Because these policing techniques are hierarchical in nature (bandwidth can be first policed between users and then policed again between services to a particular user), the feature is called SSG Hierarchical Policing.

## Transparent Passthrough

The Transparent Passthrough feature allows unauthenticated traffic to pass through an interface. Interfaces configured as transparent passthrough are treated as Cisco IOS interfaces and not SSG interfaces. The Cisco 10000 series Internet router can receive transparent passthrough traffic on both the access side and the network side. When an interface is configured as transparent passthrough, SSG does not process the traffic to and from the interface or apply SSG features. Instead, Cisco IOS software processes the traffic and applies Cisco IOS features.

## Multicast Protocols on SSG Interfaces

SSG supports multicast traffic, which includes normal multicast packets and Internet Group Management Protocol (IGMP) packets. The multicast traffic is separate from the SSG traffic and is routed through normal Cisco IOS processing and features; it is not routed through SSG authentication or features such as per-service statistics or hierarchical policing.

## SSG TCP Redirect

The SSG TCP Redirect feature redirects certain user packets to an alternative location that can handle the packets in a suitable manner. This feature works in conjunction with the SESM web interface. SSG TCP Redirect forces subscribers to authenticate before accessing the network or specific services and ensures that subscribers are only allowed to access the services that the service provider wants them to.

The SSG TCP Redirect feature supports the following:

- Redirection for unauthenticated users
- Redirection for unauthorized services
- Initial captivation

For more information, refer to the “Service Selection Gateway” chapter in the [Cisco 10000 Series Internet Router Service Selection Gateway Configuration Guide](#).

## VPI/VCI Static Binding to a Service Profile

The VPI/VCI Static Binding to a Service Profile feature allows users accessing SSG through a VPI/VCI or a range of VPI/VCI to access the server. When a user session arrives on a VPI/VCI or a VPI/VCI range and the session specifies the username but does not specify the domain name, SSG maps the user session to the service to which the VPI/VCI or VPI/VCI range is bound.

## RADIUS Virtual Circuit Logging

RADIUS Virtual Circuit (VC) Logging extends and modifies the RADIUS network access server (NAS) port field to carry VPI/VCI information. With RADIUS VC Logging enabled, the Cisco 10000 Internet router (the SSG node) can send NAS port information to the RADIUS server, accurately recording the virtual path interface (VPI) and virtual circuit interface (VCI) of an incoming user or subscriber session. The VPI/VCI of the incoming permanent virtual circuit (PVC) is recorded at the point of entry on SSG, which offers the RADIUS client a unique VPI/VCI for each incoming PVC. This information is logged in the RADIUS accounting record that was created at session startup.

## AAA Server Group Support for Proxy Services

The AAA Server Group Support for Proxy Services feature allows you to configure multiple AAA servers for redundancy. The RADIUS Server attribute enables AAA server group support for proxy services. Each group is associated with a service that requires proxy RADIUS AAA. You can configure each remote RADIUS server with timeout and retransmission parameters. When necessary, the SSG performs failover among the servers in the predefined group.

## Packet Filtering

The Cisco 10000 series Internet router supports per-user access control lists (ACLs) to prevent users from accessing specific IP addresses and ports. When an ACL attribute is added to a user profile, the attribute applies globally to all the user's traffic.

SSG accepts Cisco IOS ACLs and SSG ACLs. SSG ACLs take precedence over Cisco IOS ACLs when both Cisco IOS and SSG ACLs are configured on the same SSG interface.

An SSG ACL can have a maximum of 8 access-list entries (ACEs). If you use the TCP Redirect feature, TCP Redirect uses one of the 8 ACEs; therefore, you can configure only 7 ACEs.

## SSG Unconfig

The SSG Unconfig feature enhances your ability to disable SSG at any time and releases the data structures and system resources created by SSG when SSG is unconfigured.

SSG Unconfig removes SSG allocated resources when you globally disable SSG after it was enabled. When you enable SSG, the SSG subsystem in the Cisco IOS software acquires system resources that are never released, even after you disable SSG. The SSG Unconfig feature enables you to release and clean up system resources when SSG is not in use.

## Per-Service Statistics

The Cisco 10000 series Internet router collects statistics about router interfaces and the connections to them in both the input and output directions. Cisco CLI commands, such as **show interface**, are used to display information about the interfaces. SSG commands, such as **show ssg connection**, are used to display information about the connection to the router.

## Field Diagnostics

Field Diagnostics provides customers with a method of testing and verifying line card hardware problems.

If you would like to perform a hardware diagnostic test on any line card in your Cisco 10000 series router, a Field Diagnostic image can be downloaded free of charge from Cisco Systems and used to test whether the line card problems are indeed due to faulty hardware. The test results will verify whether or not the hardware is faulty.

For additional information on Field Diagnostic tests, refer to the *Field Diagnostics for the Cisco 10000 Series Router* located at the following URL:

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

## 8-Port DS3/E3 ATM Line Card

The 8-port DS3/E3 ATM line card is a full height card that provides eight DS3 or E3 connections to ATM networks. The line card functionality focuses on Layer 2 ATM services and relies on the performance routing engine (PRE, Part Number ESR-PRE2) to provide Layer 3 services. The DS3/E3 ATM line card receives and transmits ATM cells on the physical interfaces while transmitting and receiving packets from the backplane.

The 8-port DS3/E3 ATM line card provides the following hardware features:

- 8 DS3/E3 ports on a full height, single slot line card
- Rear chassis cabling with BNC connectors
- DS3 features:
  - Per interface M23 or C-bit parity framing mode
  - Per line card DSX3 modes: T3 ADM, T3 PLCP
  - DS3 line or payload loopback
  - Internal or loop timing
  - Per interface line build out: 450 ft. of 75 ohm coaxial cable
- E3 features:
  - Per interface G.751 or G.832 framing mode
  - Per line card DSX3 modes: E3 ADM, E3 PLCP
  - E3 line or payload loopback
  - Internal or loop timing
- ATM features:
  - Supports up to 32,000 VCs per line card, maximum of 4,000 VCs per port, all 16 VCI and 8 VPI bits are available
  - Supports AAL5 data transport, F4 and F5 OAM cells
  - Per VC and per VP traffic shaping
- 64 MB packet memory in each direction

Mixing DSX3 modes on a per port basis is not supported. When you configure the 8-port E3/DS3 ATM line card for a DSX3 mode, all eight ports of the line card operate in the mode you have selected.

The DS3/E3 ATM line card supports the following throughput rates and ATM framing for the specified DSX3 modes:

DSX3 Mode	Throughput Rate	ATM Framing
T3 ADM	44200 Kbps	CBIT or M23
T3 PLCP	40700 Kbps	CBIT or M23
E3 ADM	34000 Kbps	G.751 or G.832
E3 PLCP	30600 Kbps	G.751 only

For more information, refer to the [“Configuring the 8-Port E3/DS3 ATM Line Card”](#) in the *Cisco 10000 Series Internet Router Software Configuration Guide*.

## Cisco 10000 Series Router MIB Enhancements

Cisco IOS Release 12.2(16)BX adds support for the CISCO-SSG-MIB. For more information about the MIB capabilities on the router, refer to the [Cisco 10000 Series Broadband MIB Specifications Guide](#). (Chapter 3, "MIB Specifications," lists MIBs constraints.)

## 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)

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

<b>Routing Protocols</b>	Border Gateway Protocol (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 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.

- [L2TP Tunnel Authorization, page 12](#)
- [Broadband Aggregation Groups, page 13](#)
- [ATM PXF Queuing, page 13](#)
- [Dynamic Bandwidth Selection, page 13](#)
- [QoS Service Policy on a Virtual Access Interface, page 13](#)
- [CISCO-VPDN-MGMT MIB, page 13](#)
- [AAA Method Lists, page 13](#)
- [Unshaped UBR PVCs, page 13](#)
- [Shaped UBR PVCs, page 14](#)
- [Controlling the Rate of Logging Messages, page 14](#)
- [Testing Performance of High-Speed Interfaces, page 14](#)

## L2TP Tunnel Authorization

Cisco 10000 router supports 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 ATM PXF queuing, to ensure reliable operation you must enter the **no atm pxf queuing mode** command before you configure any 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 VP tunnels.

## QoS Service Policy on a Virtual Access Interface

If you apply an output QoS service policy on a virtual-access interface, and that virtual access interface is L2TP tunneled (When the router is configured as an LNS, for example) and the service policy indicates that the TOS or 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 supports a maximum of 8000 unshaped 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 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, 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)BX:

- [Provisioning for Scaling, page 15](#)
- [Inserting a New Line Card, page 15](#)

## Provisioning for Scaling

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

- [PPPoA Sessions with IP QoS Static Routes, page 15](#)
- [AAA Authentication on the NME Port, page 15](#)
- [Call Admission Control, page 15](#)

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 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 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
```

## 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)BX

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

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

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 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>
<b>CSCea27261</b>	<p>The network access server (NAS) sends an unwanted Access request for PPP terminated aggregation (PTA).</p> <p>When you configure virtual private dial-up network (VPDN) with RADIUS, a double RADIUS lookup occurs. This decreases performance on a RADIUS server with a large number of additional RADIUS requests.</p> <p><b>Workaround:</b> None.</p>
<b>CSCea30354</b>	<p>When the 8-port DS3/E3 ATM line card is configured for DS3 ADM or DS3 PLCP DSX3 mode, and the line card is connected back-to-back with another 8-port DS3/E3 ATM line card, the DS3/E3 ATM interface on the first line card counts a large quantity of 00F events when you shut down the interface on the far-end ATM device.</p> <p><b>Workaround:</b> None.</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> None.</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> None.</p>
<b>CSCea37038</b>	<p>If APS is configured using the <b>aps force atm &lt;slot/subslot/port&gt; 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 &lt;slot/subslot/port&gt;</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 &lt;slot/subslot/port&gt;</b> command.</p>
<b>CSCea37133</b>	<p>When you configure Automatic Protection System (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)BX (continued)

Caveat	Description
CSCea41145	<p>The output of the <b>show vpdn tunnel summary</b> command fails to display tunnels that have no-session timeout (set using the <b>l2tp timeout no-session timeout never</b> command).</p> <p><b>Workaround:</b> Do not set the no session timeout to never. In the following example, the no-session timeout is set to 30:</p> <pre>router# l2tp timeout no-session 30</pre>
CSCea45943	<p>In a Cisco 10000 chassis with redundant PREs, after a switch-over 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 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 ODAP subnets allocated from the 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>
CSCea59894	<p>On the 8-port DS3/E3 ATM line card, ILMI discovery is not complete when the line card is operating in the DS3 ADM and DS3 PLCP DSX3 modes. The ILMI state remains in the WaitDevType state and the line card does not discover the adjacent ATM switch information.</p> <p>When operating in the E3 ADM and E3 PLCP DSX3 modes, the line card properly discovers the adjacent ATM switch values.</p> <p><b>Workaround:</b> None.</p>
CSCea66307	<p>When a large number (for example, 30,000) of established PPP sessions terminate at the same time, the Cisco 10000 series router can exhaust I/O memory. This causes a loss of other services such as maintaining L2TP tunnels and dropping AAA accounting requests to the RADIUS server.</p> <p><b>Workaround:</b> None.</p>
CSCea66654	<p>Channelized interfaces with 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>

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

Caveat	Description
<p><b>CSCea67815</b></p>	<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="553 489 732 510">%ALIGN-3-TRACE</pre> <p><b>Workaround:</b> None.</p>
<p><b>CSCea70951</b></p>	<p>A memory allocation error occurs when you attempt to scale a large number of users (for example, 4000 PPPoA 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>
<p><b>CSCea72016</b></p>	<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>
<p><b>CSCea73477</b></p>	<p>Packet counters and debug messages on the Cisco 10000 series router cannot be used to accurately count or view 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>
<p><b>CSCea77321</b></p>	<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>
<p><b>CSCea78861</b></p>	<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>
<p><b>CSCea78890</b></p>	<p>If you perform a <b>tftp copy</b> of a running configuration greater than 5 MB to a 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>

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

Caveat	Description
<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>CSCea82309</b>	<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> There is currently no workaround.</p>
<b>CSCeb01499</b>	<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 data-bbox="589 730 1513 835"> 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>
<b>CSCeb08194</b>	<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>
<b>CSCeb17086</b>	<p>Traceback messages appear while configuring static multicast routes.</p> <p><b>Workaround:</b> None.</p>
<b>CSCeb21692</b>	<p>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.</p> <p><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.</p>
<b>CSCeb26162</b>	<p>In some cases, while the Cisco 10000 series router terminates PPP sessions, the router delays the transmission of the RADIUS Accounting-On message for too long, thus clearing the accounting data on the RADIUS server about the sessions that are already established.</p> <p><b>Workaround:</b> Reset the PPPoX clients that connect too early.</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> None.</p>
<b>CSCeb30288</b>	<p>The Cisco 10000 series router might be delayed executing the <b>reload</b> command if AAA accounting configured. During this time packets are <i>not</i> forwarded.</p> <p><b>Workaround:</b> None.</p>

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

<b>Caveat</b>	<b>Description</b>
<b>CSCeb31498</b>	<p>When Dynamic Bandwidth Selection (DBS) is enabled on a VC class, DBS fails and displays the following error message:</p> <pre>Jun 5 13:21:19.200: %C10K DBS: validate_params() 2/111, vcd 11, QoS type 5, PCR 50, SCR 38</pre> <pre>Jun 5 13:21:19.200: %C10K DBS: validate() QoS update rejected PVC 2/111 on VP tunnel</pre> <p><b>Workaround:</b> None.</p>
<b>CSCeb33056</b>	<p>The Cisco 10000 series router frequently displays the following 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> None.</p>
<b>CSCeb35104</b>	<p>Configurations with a very large number of subinterfaces (for example, 32,000) might experience slow PPPoEa session clearing.</p> <p><b>Workaround:</b> None.</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 pvc-in-range 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> None.</p>
<b>CSCeb38277</b>	<p>When an ATM interface is configured as unnumbered, the Cisco 10000 series router does not forward RBE traffic to RBE clients.</p> <p><b>Workaround:</b> None.</p>
<b>CSCeb39292</b>	<p>The Cisco 10000 series router is sometimes unable to sync the configuration between the active and standby performance routing engine (PRE).</p> <p><b>Workaround:</b> None.</p>
<b>CSCeb41285</b>	<p>The Cisco 10000 series router does not create the virtual access interface (VAI) if the RADIUS user profile includes Frame-Compression AVP. If the AVP for compression is removed from the user profile, the router creates the VAI.</p> <p><b>Workaround:</b> Do not specify framed-compression none in RADIUS profiles.</p>
<b>CSCeb42938</b>	<p>The following traceback message randomly appears:</p> <pre>00:48:42: %AAA-3-BADMETHOD: Cannot process authorization method 1635568848</pre> <pre>-Process= "AAA Server", ipl= 0, pid= 58</pre> <pre>-Traceback= 603B6A1C 603AFE24 603B0C58 603B0D78</pre> <p><b>Workaround:</b> None.</p>

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

Caveat	Description
<b>CSCeb44881</b>	<p>When you run L2TP-related tests on the Cisco 10000 series router using Adtech AX4000 automation scripts, the following traceback messages might appear in the log:</p> <pre>*Jun 19 18:28:23.103: %GENERAL-3-EREVENT: Invalid entry Cached -Traceback= 60BF56F4 60BF6174 60AC88F8 60A6F5C4 60A8E894 60A929FC 60A8CC54 60A8D590</pre> <p><b>Workaround:</b> None.</p>
<b>CSCeb48599</b>	<p>PPPoE accounting does not work properly for PPP termination and L2TP forwarding when the client uses PPPoE. The Cisco 10000 series router accounts for more packets than are actually sent or received.</p> <p><b>Workaround:</b> None.</p>
<b>CSCeb48677</b>	<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>
<b>CSCeb49776</b>	<p>Multiple memory leaks occur while testing the Cisco IOS Release 12.2(16)BX image.</p> <p><b>Workaround:</b> None.</p>
<b>CSCeb50036</b>	<p>The first time PPPoX sessions with an access control list (ACL) applied by a virtual template arrive at the Cisco 10000 series router, the router applies the ACL to the sessions and establishes the sessions as expected. However, after the performance routing engine (PRE) fails over to the redundant PRE or after a session disconnects and then reconnects with a large number of sessions, the Cisco 10000 series router attempts to apply the ACL before the session is established, which causes the following error message to appear:</p> <pre>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</pre> <p>After the Cisco 10000 series router establishes the sessions, the router applies the ACL as expected and the ACL is in effect.</p> <p><b>Workaround:</b> None.</p>
<b>CSCeb51308</b>	<p>When 61,500 PPPoEoA sessions are active and SNMP is running in the background, executing the <b>show ios</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>

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

Caveat	Description
<b>CSCeb51344</b>	<p>RADIUS configurations that use <b>lcp:</b> in the vendor specific attributes (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 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>
<b>CSCeb52236</b>	<p>When using the 8-port DS3/E3 ATM line card, PVCs discovered by ILMI can occasionally experience lower than expected throughput performance.</p> <p><b>Workaround:</b> None.</p>
<b>CSCeb52243</b>	<p>On the 8-port DS3/E3 ATM line card, F5 OAM Rate Limiting does not properly drop the OAM cells that exceed the rate limit.</p> <p><b>Workaround:</b> None.</p>
<b>CSCeb53208</b>	<p>The Cisco 10000 router creates PPP sessions without allocating a VCCI.</p> <p><b>Workaround:</b> None.</p>
<b>CSCeb53344</b>	<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>
<b>CSCeb53380</b>	<p>Under some conditions, the call setup rate might be less than the rate achieved with Cisco IOS Release 12.2(15)BX.</p> <p><b>Workaround:</b> None.</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> None.</p>
<b>CSCeb54544</b>	<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>
<b>CSCeb54587</b>	<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>

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

Caveat	Description
<b>CSCeb55625</b>	<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 data-bbox="589 426 1513 636">*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 &lt;slot #&gt;</b> command. You can then insert the 1-port OC-12 POS line card into the chassis.</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> None.</p>

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

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

### CSCdu53656

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

### CSCea28131

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

**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 online insertion and removal (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 access control lists (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 virtual path (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 network access server (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 virtual access interface (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 performance routing engine (PRE) is executed. This has been fixed.

**CSCeb39442**

The Cisco 10000 series router does not update the QoS shaping parameters for a VC when Dynamic Bandwidth Selection (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.

## 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 L2TP network server (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, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, 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 United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

Copyright © 2003–2004 Cisco Systems, Inc. All rights reserved.