



Release Notes for the Cisco 10000 Series Router for Cisco IOS Release 12.2(16)BX3

May 10, 2004

Cisco IOS Release 12.2(16)BX3

These release notes for the Cisco 10000 series router support Cisco IOS Release 12.2(16)BX3, 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.

We recommend 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. 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.

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 8](#)
- [Important Notes, page 11](#)
- [Caveats for Cisco IOS Release 12.2\(16\)BX3, page 15](#)
- [Related Documentation, page 27](#)
- [Obtaining Documentation, page 27](#)
- [Documentation Feedback, page 28](#)
- [Obtaining Technical Assistance, page 28](#)
- [Obtaining Additional Publications and Information, page 30](#)



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)BX3 is based on the following releases:

- Cisco IOS Release 12.2(16)BX2
- 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/ios122/122relnt/xprn122/index.htm>

System Requirements

Cisco IOS Release 12.2(16)BX3 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

New and Changed Information

The “[New Features—Cisco IOS Release 12.2\(16\)BX3](#)” section on page 3 lists the new software features supported by the Cisco 10000 series router for Cisco IOS Release 12.2(16)BX3.

For information about new features supported on the Cisco 10000 router in other 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>

New Features—Cisco IOS Release 12.2(16)BX3

The following new features are supported on the Cisco 10000 router in Cisco IOS Release 12.2(16)BX3:

- [Variable Bit Rate-Non-Real Time Oversubscription](#), page 3
- [F4 Operations, Administration, and Maintenance Ping Without Virtual Path](#), page 3
- [Non-SSG User-to-SSG User Policing](#), page 4
- [SSG Link Redundancy](#), page 6
- [Volume-Based SSG Prepaid](#), page 7

Variable Bit Rate-Non-Real Time Oversubscription

The Variable Bit Rate Non-Real Time (VBR-nrt) Oversubscription feature enables service providers to improve network utilization of otherwise underutilized shared networks by leveraging statistical multiplexing on ATM networks. Instead of supporting only unconditional reservation of network bandwidth to VCs, the router offers VC oversubscription to statistically guarantee bandwidth to VCs.

For more information, see the [Variable Bit Rate-Non-Real Time Oversubscription, Release 12.2\(16\)BX3 feature module](#) at the following URL:

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

F4 Operations, Administration, and Maintenance Ping Without Virtual Path

The F4 Operations, Administration, and Maintenance (OAM) Ping without Virtual Path (VP) Creation feature enables you to determine problems at the virtual path (VP) level using the **ping** command. Using this feature, you can create and remove virtual circuit identifiers (VCIs) that correspond to the VP segment and the VP end. These special VCs can be configured only on the Cisco 10000 router and are not available on any other Cisco platform. After creating the VCIs you can use the **ping atm** command to isolate connection problems.

For more information, see the following documents:

- [OAM on ATM Interfaces FAQs](#)
- [Using OAM for PVC Management](#)

Configuring F4 OAM Ping Without VC Creation

To configure an F4 VC segment or end, enter the following commands in interface configuration mode:

Command	Purpose
Router(config-if)# pvc VPI/3 f4-oam	Creates an F4 segment VC. <i>VPI</i> is the virtual path identifier value. Valid values are from 0 to 255.
Router(config-if)# pvc VPI/4 f4-oam	Creates an F4 end VC. <i>VPI</i> is the virtual path identifier value. Valid values are from 0 to 255.

Verifying F4 VC Segment and End Creation

To verify the creation of an F4 VC segment or end, enter the following commands in privileged EXEC mode:

Command	Purpose
Router# <code>show atm pvc VPI/3</code>	Displays information about the F4 segment VC. <i>VPI</i> is the virtual path identifier value. Valid values are from 0 to 255.
Router# <code>show atm pvc VPI/4</code>	Displays information about the F4 VC end. <i>VPI</i> is the virtual path identifier value. Valid values are from 0 to 255.

Configuration Example for F4 VC Creation

The following example shows how to create an F4 segment VC with a VPI/VCI pair of 10 3:

```
pvc 10/3 f4-oam
```

The following example shows how to create an F4 end VC with a VPI/VCI pair of 10 4:

```
pvc 10/4 f4-oam
```

The following example shows how to ping the newly created F4 segment and end VCs:

```
ping atm interface atm1/1 10 3
ping atm interface atm1/1 10 4
```

Non-SSG User-to-SSG User Policing

The Non-SSG User-to-SSG User Policing feature controls user-to-user traffic by policing aggregated traffic destined to or sent from a particular host. Using this feature, you can configure a policing rate for the upstream, downstream, or both upstream and downstream traffic for SSG hosts.



Note

This feature is available only on the Cisco 10000 series router. It is not available on other Cisco SSG platforms.

When you configure the Non-SSG User-to-SSG User Policing feature, the Cisco 10000 router determines the policing rate for the SSG host based on the sum of the rate that you specify and the aggregate rate of the services to which a user is subscribed. If you specify a rate of 0, the Cisco 10000 router uses only the sum of the user-subscribed services to calculate the policing rate. The non-SSG user-to-SSG user policer is a global policer; therefore, applying this policer places a policing rate on all subscribers.

If you configure a per-subscriber host policing rate and a non-SSG user-to-SSG user policing rate, the per-subscriber host rate overrides the non-SSG user-to-SSG user policing rate and is applied for a host.

Configuring Non-SSG User-to-SSG User Policing

To configure a non-SSG user-to-SSG user policer, enter the following command in global configuration mode:

Command	Purpose
<pre>Router(config)# pxf ssg host {upstream downstream} [base_rate]</pre>	<p>Configures the policing rate that you specify for traffic to and from a particular SSG host.</p> <p>(Optional) The <i>base_rate</i> parameter is the minimum bandwidth required. The Cisco 10000 uses this rate to derive the policing rate for traffic for the SSG host. Valid values are numbers from 0 to 2,500,000,000. The default value is 0.</p> <p>Note You can configure a policer for the upstream, downstream, or both the upstream and downstream traffic for SSG hosts.</p>

Configuration Example for Both Upstream and Downstream Policing

Scenario

User A is subscribed to the BasicA service at a rate of 256 Kbps downstream and 128 Kbps upstream.

Configuration Example

The following example configures both upstream and downstream policing at a rate of 64 Kbps:

```
pxf ssg host upstream 64
pxf ssg host downstream 64
```

Policing Calculations

The Cisco 10000 router determines the policing rate to apply to the downstream and upstream traffic for SSG hosts using the following calculations:

- Downstream traffic—64 Kbps + 256 Kbps = 320 Kbps
- Upstream traffic—64 Kbps + 128 Kbps = 192 Kbps

If the SSG host attempts to access peer-to-peer applications, the Cisco 10000 router limits the bandwidth of the downstream traffic to 320 Kbps and the upstream traffic to 192 Kbps.

If the host attempts to simultaneously access the Internet and peer-to-peer applications, the router still limits the total bandwidth for peer-to-peer applications to 320 Kbps downstream and 192 Kbps upstream, and the router limits the Internet bandwidth to 256 Kbps downstream and 128 Kbps upstream.

Configuration Example for Both Upstream and Downstream Policing at a Specified Rate of 0

Scenario

UserA is subscribed to the BasicA service at a rate of 256 Kbps downstream and 128 Kbps upstream.

UserB is subscribed to the BasicA service at a rate of 256 Kbps downstream and 128 Kbps upstream, and to the Video service at a rate of 1 Mbps downstream and 128 Kbps upstream.

UserC is subscribed to the BasicA service at a rate of 256 Kbps downstream and 128 Kbps upstream, and to the Video service at a rate of 1 Mbps downstream and 128 Kbps upstream. UserC has a host-based policing rate configured using SESM.

Configuration Example

The following example configures both upstream and downstream policing at a specified rate of 0:

```
pxf ssg host upstream 0
pxf ssg host downstream 0
```

Policing Calculations for UserA

The Cisco 10000 router determines the policing rate to apply to the downstream and upstream traffic for SSG hosts using the following calculations:

- Downstream traffic—0 Kbps + 256 Kbps = 256 Kbps
- Upstream traffic—0 Kbps + 128 Kbps = 128 Kbps

If the SSG host accesses peer-to-peer applications, the router limits the bandwidth to 256 Kbps downstream and 128 Kbps upstream. If the host simultaneously accesses the Internet and peer-to-peer applications, the router still limits the total bandwidth to 256 Kbps downstream and 128 Kbps upstream.

Policing Calculations for UserB

The Cisco 10000 router determines the policing rate to apply to the downstream and upstream traffic for SSG hosts using the following calculations:

- Downstream traffic—256 Kbps + 1 Mbps = 1.256 Mbps
- Upstream traffic—128 Kbps + 128 Kbps = 256 Kbps

If the SSG host accesses peer-to-peer applications, the router limits the bandwidth to 1.256 Mbps downstream and 256 Kbps upstream. If the host simultaneously accesses the Internet, video, and peer-to-peer applications, the router still limits the total bandwidth to 1.256 Mbps downstream and 256 Kbps upstream. The router also limits the Internet bandwidth to 256 Kbps downstream and 128 Kbps upstream, and Video bandwidth to 1 Mbps downstream and 128 Kbps upstream.

Policing Calculations for UserC

Because UserC has a host-based policing rate configured using SESM, the router uses the SESM policing rate as the SSG host rate.

SSG Link Redundancy

The SSG Interface Redundancy feature enables providers to configure the Cisco Service Selection Gateway (SSG) with redundant uplink interfaces to services and to the default network. This feature also supports the configuration of redundant downlink interfaces for nonoverlapping users configured with the port-bundle host key functionality. Interface redundancy benefits service providers as well as subscribers by helping to prevent subscriber downtime due to interface failure.

For more information, see the [SSG Link Redundancy, Release 12.2\(16\)BX3 feature module](#).

Volume-Based SSG Prepaid

The SSG Prepaid feature allows a user to connect to a service if the user has prepaid for the service. 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, which are allotments of available credit.

The volume-based SSG Prepaid feature allows for real-time billing with maximum flexibility, regardless of the type of service and billing scheme. Users are billed on a volume basis. The quotas represent the allowable data volume, expressed in bytes. Volume quotas are for combined upstream and downstream traffic.

To obtain the first quota for a connection, SSG submits an authorization request to the AAA server. The AAA server contacts the prepaid billing server, which forwards the quota values to SSG. SSG then monitors the connection to track the quota usage. When the quota runs out, SSG performs reauthorization. During reauthorization, the billing server can provide SSG with an additional quota if there is available credit. If no further quota is provided, SSG logs off the user.

For the Cisco 10000 router, it can take up to one minute to detect that the volume-based prepaid quota has expired. The SSG Prepaid feature accounts the excess quota used in the current period against the quota received from the next prepaid reauthorization.

A Quota VSA in the RADIUS access-accept packet defines the quota parameters for a connection. [Table 1](#) defines the Quota VSA.

Table 1 Quota VSA

Attribute ID	Vendor ID	Subattribute ID and Type	Attribute Name	Subattribute Data
26	9	253 Control-Info	Quota	Q—Control-Info code for prepaid quota. T or V—Quota subcode for time or volume. <i>numeric string</i> —Quota value.

For more information, see the [Cisco 10000 Series Router Service Selection Gateway Configuration Guide](#) and the [SSG Prepaid, Release 12.2\(4\)B](#) feature module.

Configuring Volume-Based SSG Prepaid

To configure SSG to provide the prepaid billing server with the session ID and volume-based information, enter the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# radius-server attribute 55 include-in-acct-req	Sends the RADIUS attribute 55 (Event-Timestamp) in the accounting packets.
Step 1	Router(config)# radius-server attribute 44 include-in-access-req	Sends the RADIUS attribute 44 (Acct-Session-ID) in the access-request packets before performing user authentication (including requests for preauthentication).
Step 2	Router(config)# radius-server vsa send authentication	Configures the network access server to recognize and use vendor-specific authentication attributes.

Configuration Example for Volume-Based SSG Prepaid

The following example displays information about the SSG connection for a prepaid service that uses a volume-based quota:

```
Router# show ssg connection 10.1.1.19 InstMsg

-----ConnectionObject Content-----

User Name:
Owner Host:10.1.1.19
Associated Service:InstMsg
Connection State:0 (UP)
Connection Started since:*00:25:58.000 UTC Tue Oct 23 2003
User last activity at: *00:25:59.000 UTC Tue Oct 23 2003
Connection Traffic Statistics:
    Input Bytes = 0, Input packets = 0
    Output Bytes = 0, Output packets = 0
    Quota Type = 'VOLUME', Quota Value = 100
Session policing disabled
```

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 8](#)
- [L2TP Tunnel Authorization, page 9](#)
- [Broadband Aggregation Groups, page 9](#)
- [ATM PXF Queuing, page 9](#)
- [Dynamic Bandwidth Selection, page 9](#)
- [QoS Service Policy on a Virtual Access Interface, page 9](#)
- [CISCO-VPDN-MGMT MIB, page 9](#)
- [AAA Method Lists, page 10](#)
- [Unshaped UBR PVCs, page 10](#)
- [Shaped UBR PVCs, page 10](#)
- [Controlling the Rate of Logging Messages, page 10](#)
- [Testing Performance of High-Speed Interfaces, page 10](#)

ssg bind direction Command Not Supported

Instead of the **ssg bind direction** command, which returns 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 about 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)BX3:

- [Interoperability with Test Equipment, page 11](#)
- [Provisioning for Scaling, page 11](#)
- [Enhancing Scalability of Per-User Configurations, page 13](#)
- [Inserting a New Line Card, page 15](#)
- [Multilink PPP, page 15](#)

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:

- [PPP Terminated Aggregation Session Scaling, page 12](#)
- [CISCO-ATM-PVCTRAP-EXTN-MIB, page 12](#)
- [PPPoA Sessions with IP QoS Static Routes, page 13](#)
- [AAA Authentication on the NME Port, page 13](#)
- [Call Admission Control, page 13](#)

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, see the [Cisco 10000 Series Router Broadband Aggregation Configuration Guide](#).

PPP Terminated Aggregation Session Scaling

CSCee24114

PPP terminated aggregation (PTA) sessions sometimes do not scale as expected because automatic PPP messages are saved to the buffer, which can cause PTA call rates to degrade. To avoid this problem, add the following command to the router's configuration:

Command	Purpose
Router(config)# logging buffered warnings	Limits the logging of messages to the local buffer to warning conditions (level 4).

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)# snmp-server view <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 included 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)# snmp-server view <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)# snmp-server community <i>string [view view-name] [ro rw]</i> [access-list-number]	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 must only specify 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.

Each time 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

Multilink PPP

Multilink PPP (MLPPP) is not supported on Cisco IOS Release 12.2(16)BX3.

Caveats for Cisco IOS Release 12.2(16)BX3

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 sections.

For information about caveats in Cisco IOS Release 12.2(16)BX3, see the following sections:

- [Open Caveats—Cisco IOS Release 12.2\(16\)BX3, page 16](#)
- [Resolved Caveats—Cisco IOS Release 12.2\(16\)BX3, page 18](#)
- [Other Caveats, page 26](#)

Open Caveats—Cisco IOS Release 12.2(16)BX3

Table 2 describes open caveats in Cisco IOS Release 12.2(16)BX3.

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 2 Open Caveats in Cisco IOS Release 12.2(16)BX3

Caveat	Description
CSCdy79740	<p>If 32,000 PPPoA sessions, 99 VRFs, RADIUS authentication, and the per vrf aaa case 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>Workaround: 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 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.</p> <p>Workaround: There is no workaround for this problem.</p>
CSCea52741	<p>If the Cisco 10000 series router reloads unexpectedly, any On-Demand Address Pool (ODAP) subnets allocated from the Cisco Network Registrar (CNR) remain marked as Leased (at the CNR).</p> <p>Workaround: 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>
CSCea67815	<p>When you disable 32,000 sessions over 10,000 L2TP tunnels on a Cisco 10000 series router configured as an LNS with RADIUS AAA accounting enabled, the router might terminate the remaining sessions due to the overwhelming number of RADIUS records generated by this event. If this occurs, the following message might appear on the console:</p> <pre>%ALIGN-3-TRACE</pre> <p>Workaround: There is no workaround for this problem.</p>
CSCea72016	<p>The channelized OC-12 line card undergoes a watchdog reset when unconfiguring six channelized OC-12 line cards set up with 768 T1s each. This occurs only with a very specific large channelized card setup. This does not occur with five or less channelized OC-12 line cards.</p> <p>Workaround: Unconfigure fewer OC-12 channelized interfaces at one time.</p>
CSCea81015	<p>If you configure the management Ethernet port (fastethernet 0/0/0) on the PRE (part number ESR-PRE2) front panel using the ip address dhcp command, the port does not acquire an IP address.</p> <p>Workaround: Configure the fastethernet 0/0/0 interface with a static IP address.</p>

Table 2 Open Caveats in Cisco IOS Release 12.2(16)BX3 (continued)

Caveat	Description
CSCeb01499	<p>The following traceback message displays in the log after you enter the hardware subslot shutdown, no card, and no hardware subslot shutdown or card 24che1t1 mode t1 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>Workaround: There is no workaround for this problem.</p>
CSCeb26165	<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 reload command.</p> <p>Workaround: There is no workaround for this problem.</p>
CSCeb51344	<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>Workaround: There is no workaround for this problem.</p>
CSCeb53474	<p>With TACACS configured on the Cisco 10000 series router, the secondary PRE (part number ESR-PRE2) console attempts TACACS authentication using the fa0/0/0 interface. Before notifying the user that the secondary console is unavailable, the secondary PRE incorrectly attempts to contact the TACACS server for user authentication. The secondary PRE should not attempt to contact the TACACS server or it should try to contact the TACACS server using the primary PRE.</p> <p>Workaround: There is no workaround for this problem.</p>
CSCec24597	<p>When configuring a constant bit rate permanent virtual circuit (CBR PVC) using a test script, a traceback message appears and the router does not create the CBR PVC.</p> <p>Workaround: There is no workaround for this problem.</p>
CSCed91686	<p>When a nested policy map is attached to a subinterface, deleting the subinterface generates continuous traceback messages, and the router becomes unstable.</p> <p>Workaround: There is no workaround for this problem.</p>
CSCee03702	<p>A Cisco 10000 router with dual performance routing engines (PREs, part number ESR-PRE2) and dual route processors (RPs) fails at GetHostKey_10HostObjectP7hostkey.</p> <p>Workaround: There is no workaround for this problem.</p>
CSCee40092	<p>If you issue a shut/no shut command sequence while configured MPP bundles are carrying traffic, this triggers the race condition when MLP bundles are coming back up. MLP bundles fail to come up successfully because of a lack of resources for the bundle.</p> <p>Workaround: There is no workaround for this problem.</p>

Table 2 Open Caveats in Cisco IOS Release 12.2(16)BX3 (continued)

Caveat	Description
CSCee42660	When you implement auto-vc configuration using the pvc-in-range command and change the value of the class-vc to a different UBR+ speed, a traceback message appears. The PVC can enter a blocked state and the router can stop responding. Workaround: There is no workaround for this problem.
CSCee49305	If you issue the no shut command on a configured MLP bundle that is already in an UP/UP state, the MLP bundle and member interface link bounce each time. When an interface is in an UP/UP state, a no shut command should not bounce the interface. Workaround: There is no workaround for this problem.
CSCee51262	If you configure the clock source as line on a channelized STM1 line card on a Cisco 10000 series router, line flaps occur. This problem occurs only when there is an SDH network in the middle. Back-to-back configurations do not show this problem on a PRE, part number ESR-PRE2. Workaround: Configure the clock source line command one time.
CSCin46447	When you disable SSG traffic policing on the router by entering the no ssg qos police user and the no ssg qos police session commands, the router continues to police the traffic for the existing host and connection. Workaround: There is no workaround for this problem.

Resolved Caveats—Cisco IOS Release 12.2(16)BX3

This section describes caveats that were fixed in Cisco IOS Release 12.2(16)BX3.

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>

CSCea35508

(Duplicate of CSCea45943, CSCea46076) The throughput of Frame Relay traffic was sometimes up to 5 percent lower than the maximum possible throughput. This has been fixed.

CSCea37019

The Cisco 10000 series router displayed a bus fault error when automatic protection switching (APS) was configured on the OC-12 ATM line card. This has been fixed.

CSCea37038

(Duplicate of CSCeb15960) If APS was configured using the **aps force atm slot/subslot/port from protect** command on the 4-port OC-3 line card or the single-port OC-12 ATM line card, and a signal failure was received on the port of either line card, the output of the **show interface atm slot/subslot/port** command sometimes indicated the interface was up instead of down. This has been fixed.

CSCea37133

(Duplicate of CSCea45002) When you configured automatic protection switching (APS) switchover on the 4-port OC-3 ATM line card, entering the **show controller atm slot/subslot/port** command for the ATM port displayed a signal degrade status for both the protection port and the working port. This has been fixed.

CSCea45943

(Duplicate of CSCeb73578) 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 was low. This has been fixed.

CSCea50276

(Duplicate of CSCea35065, CSCea55991) When you entered the **show processes memory sorted** command in privileged EXEC mode, the software sometimes forced the router to reload. This has been fixed.

CSCea70951

A memory allocation error occurred when you attempted to scale a large number of users (for example, 4,000 PPPoA Service Selection Gateway [SSG] sessions). All of the connections were established and the **show ssg** command displayed all of the sessions as logged in and active. However, when sessions were dropped, a memory allocation error appeared. This has been fixed.

CSCea73477

Packet counters and debug messages on the Cisco 10000 router could not be used to accurately count or view Interim Local Management Interface (ILMI) keepalive messages. This was because basic ILMI configurations generated bursts of ILMI transactions between the Cisco 10000 router and adjacent ATM switches.

For example, if you connected an OC-3 ATM line card that was installed in a Cisco 10000 router to a Cisco LS1010 ATM switch, and you enabled debugging using the **debug atm ilmi** command, the packet counters for the ILMI PVC incremented to match the bursts of packets. This is expected behavior.

CSCea78861

(Duplicate of CSCec71974) If you entered the **ip verify unicast rpf** command for a virtual template, the calls-per-second rate was reduced. This has been fixed.

CSCea84387

The Cisco 10000 router became unresponsive when multiple users simultaneously entered modular QoS CLI (MQC) commands (such as the **show policy map** command) on the same router using separate VTY sessions. This has been fixed.

CSCeb33056

The Cisco 10000 router frequently displayed the following interprocess communications (IPC) queue full message. This has been fixed.

```
00:15:49: %IPCGRP-6-NBLKCMD_Q_FULL: Nonblocking IPC command queue full (60 commands) <---
```

CSCeb35104

Configurations with a large number of subinterfaces (for example, 32,000) sometimes experienced slow PPP over Ethernet over ATM (PPPoEoA) session clearing. This has been fixed.

CSCeb36330

(Duplicate of CSCeb38165) When a range of VCs were configured for autoprovisioning, if you shut down one of the VCs in the range by using the **pvc-in-range** command, the following message scrolled on the console until you started the VC again. This has been fixed.

```
Jun 11 09:09:33.215: %ATM-5-UPDOWN: Interface ATM3/0/0.100, Changing autovc 3/101 to ADMIN_DOWN
```

CSCeb53208

The Cisco 10000 router created PPP sessions without allocating a virtual circuit connection identifier (VCCI). This has been fixed.

CSCeb62802

The ATM interface MAC address was used as the source MAC address. If RBE was also configured on the same interface with PPPoE, problems occurred at the customer premise equipment (CPE) because RBE also used the ATM interface MAC address. A customer-requested feature now provides the ability to choose the desired MAC address as the source MAC address for PPPoEoA.

CSCec23078

The parallel express forwarding (PXF) engine sometimes failed due to invalid commands being issued to the PXF. This occurred when an L2TP Network Server (LNS) received a large IP packet from the IP cloud, the destination IP address was a PPP session to a DSL customer, and the NetFlow Analyzer was enabled on the ingress interface. The size of the packet received from the trunk and entering the L2TP tunnel had to exceed the tunnel minimum transmission unit (MTU) so that fragmentation occurred. This has been fixed.

CSCec61602

A memory leak occurred when a large number of SSG users were logged in and SSG accounting was enabled. Using the **show memory summary** command, the number of free bytes for processor and I/O memory diminished rapidly. With 32,000 sessions, the memory diminished to zero after approximately 24 hours. This has been fixed.

CSCec67879

Some PPP sessions did not become active and remained in the link control protocol (LCP) negotiation state. This has been fixed.

CSCec79539

Packets became stuck in the PAK_priority queue when an interface was congested. This occurred when the default queue (without a service policy applied) received a constant stream of large packets that overburdened the default queue. The PAK_priority queue stopped dequeuing packets, which resulted in the interface going down. This has been fixed.

CSCed25284

Executing the **show facility-alarm status** command while an ATM interface is shut down sometimes led to inaccurate output from the command. This has been fixed.

CSCed26664

The output packet counters on an interface were sometimes incorrect. Depending on the Cisco IOS release software, the counters showed either a large value or an unexpected value. This occurred after entering the **clear counters** command to clear the interface counters and then entering the **microcode reload pxf** command to reload the PXF microcode. The output packet counters became corrupted. This has been fixed.

CSCed03002

An IP receive access control list (ACL) did not filter traffic when it was configured for the first time. After the ACL was removed and then configured again, the ACL started to work and filtered exactly the same traffic. This has been fixed.

CSCed43472

For SSG hosts that were connected by an ATM multipoint interface (for example, PPPoE over ATM or RFC 1483), the network access server (NAS) port information was not included in Attribute 44 (Account Session ID) in the RADIUS accounting records. This occurred even though the **radius-server attribute nas-port format d** command had been configured on the router. This has been fixed.

CSCed48941

A Cisco MGX 8800 series Route Processor Module XF (RPM-XF) sometimes failed and generated the following error message. This occurred when you entered the **clear interface sw1** command multiple times on an RPM-XF. The RPM-XF was functioning as a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). This has been fixed.

```
No memory for XCM tempbuffer logged
```

CSCed51703

When using the **police** command in a QoS policy, QoS police statistics displayed incorrectly. The values of the packet and byte counters were large and inaccurate. This has been fixed.

CSCed55518

A small memory leak occurred on the Cisco 10000 router when testing the router as a PPP terminated aggregator (PTA). This occurred when PPPoE sessions connected to and disconnected from the router. The number of sessions remained constant on the router, but memory slowly began to decrease as sessions logged on and off. This has been fixed.

CSCed57653

A flood of SSG API messages sometimes consumed all of the input/output (I/O) memory on the Cisco 10000 router. This occurred on the SSG when the remote AAA server for a RADIUS proxy service stopped responding for an extended period of time and many users tried to log in to the service. This has been fixed.

CSCed57586

The network access server (NAS) stopped accepting PPP sessions when thousands of calls were brought up and down continuously within a few days. This occurred when the virtual template interface configuration included the **ppp ipcp address unique** command. The PPP debug information included the following information. This has been fixed.

```
"IPCP: Peer address ... in use by ...".
```

CSCed57656

Extended RADIUS reload processing sometimes occurred when you changed the router configuration to use a different, inaccessible RADIUS server and then you reloaded the system. If the system had redundant route processors (RPs) and the RADIUS reload process lasted more than a couple of minutes, then the reload process sometimes allowed the redundant RP to become active before the reload process completed, which led to an erroneous switchover operation instead of the intended reload operation. The switchover operation sometimes included interprocess communications (IPC) problems, causing the system to operate incorrectly. This has been fixed.

CSCed59577

During periods of high calling rates, the router failed to apply a per-user access control list (ACL) to a virtual access subinterface and the following traceback message appeared. This has been fixed.

```
Traceback Trying to unassign never Turbod ACL.
```

CSCed61167

When you removed a multilink PPP (MLP) bundle by removing the member interface's channel information instead of by using the proper configuration removal procedure, a leak occurred in bundle resources. As a result, the resource sometimes indicated that it was no longer available and the following messages displayed in the log file. This has been fixed.

```
%GENERAL-6-INFOEVENT: No room left in Reassembly Table
%GENERAL-6-INFOEVENT: Reassembly Table request exceeded free buffer size
```

CSCed65096

A Cisco 10000 router with two redundant performance routing engines (PREs), part number ESR-PRE2, reported a bus error (instead of a multibit ECC error) before transferring control to the secondary PRE. The multibit memory hardware error occurred in the external column memory (XCM). This has been fixed.

CSCed66001

When issuing the **ping** command or sending L2TP traffic across a multiprotocol label switching (MPLS) interface with labeling enabled, MPLS encapsulated IP packets were not fragmented and the following error message appeared in the console log file. This has been fixed.

```
%LINK-4-TOOBIG
```

CSCed76717

A configuration with a policing service policy that was attached to an ATM PVC that was never operationally active caused a row or rows to be missing from the cbQosPoliceCfgTable and cbQosPoliceStatsTable for police object types (cbQosObjectsType). This has been fixed.

CSCed84038

Traceback messages continuously appeared when attempting to install multilink queues. This has been fixed.

CSCed84157

When you removed an interface at a specific speed from a multilink interface, any attempt to add a different speed interface to the multilink interface resulted in the following error message. This has been fixed.

```
% Cannot set up this bundle link--Cannot have different bandwidth links in one bundle.
```

CSCed85139

When low-latency queuing (LLQ) was configured on a multilink interface with Link Fragmentation Interface (LFI) fragmentation and the priority queue was configured as a shaped priority queue (for example, **priority percent percent** was configured), the priority queue (PQ) behaved as an absolute PQ. To protect the other queues, you had to configure a policer in the PQ. This has been fixed.

CSCed86647

When you entered the **show aaa user all** command, the session duration time reported in accounting packets was incorrect. This occurred only when the **aaa accounting session-duration ntp-adjusted** command was configured. This has been fixed.

CSCed92793

The Cisco 10000 router sometimes failed when receiving PPPoE call rates greater than 250 calls per second (cps). This has been fixed.

CSCed92942

The LAC failed when an ATM VC went down and a PPPoA session went down before the VC changed the state to up. A queuing service policy was applied to the VC and then the client session was cleared. This occurred only if the service policy was applied to the ATM VC after the session was up. This has been fixed.

CSCee05827

Under heavy traffic conditions, if a multilink PPP (MLP) bundle flapped, sometimes the MPLS bundle was not reallocated properly and the bundle could not achieve an up state. This occurred if the bundle flapped due to entering the **shutdown** or **no shutdown** command, flapping on the peer interface, or entering the **hw-module reset** command. The log file did not indicate the error, but you could view the condition using the **show pxf cpu queue multilink<x>** command. This has been fixed.

CSCee06984

When removing a QoS child policy, a traceback message appeared. This occurred only when the policy was assigned to a subinterface. The removal of the policy resulted in a change in the traffic shaping parameter in the parent policy. This has been fixed.

CSCee08515

The Link Fragmentation Interface (LFI) feature was not fragmenting packets as expected. This has been fixed.

CSCee08622

When you configured a service policy on a multilink interface and on a serial interface, the router failed to create priority queueing (PQ) in the parallel express forwarding (PXF) engine. This has been fixed.

CSCee18808

A ping failure occurred on multilink PPP (MLP) bundles after a high availability (HA) switchover. Not all of the MLP bundles returned to the up state. This was a serialization problem with tearing down the bundle on the PRE from which the bundle was switched. This has been fixed.

CSCee19806

The Cisco 10000 router sometimes failed after the following error and traceback messages appeared on the console. This has been fixed.

```
%C10K_QUEUE_CFG_GENERAL-2-EREVENT: Error @ ../toaster/c10k_rp/c10k_tt_queue_cfg.c:3440
-Traceback= 60B9E770 60BA24EC 60BF1FDC 6007E6EC 60139650 60138A34 60C0E82C 60171404
60171540
```

CSCee25478

The pvc-in-range configuration disappeared after online insertion and replacement (OIR) of the line card. This occurred only with create on-demand VCs. This has been fixed.

CSCee25993

A Cisco 10000 router with redundant performance routing engines (PREs, part number ESR-PRE2) sometimes was not able to completely write a core dump file when required. This occurred because the secondary PRE reset the primary PRE before the file writing operation had completed. This has been fixed.

CSCee26410

When you entered the **microcode reload pxf** command on the same router or a peer router, ping failures were observed. This sometimes occurred after entering the command multiple times. This has been fixed.

CSCee26688

Entering the **shutdown** command and then the **no shutdown** command on an interface caused the following error message and traceback message to appear in the log file. This occurred when one bundle was configured with one member and no traffic was configured. This has been fixed.

```
01:19:47: %GENERAL-3-EREVENT: flushing bit is not set, cannot write to esn_word
-Traceback= 60CDA7A4 60CDB7E8 60CE04F8 60CDE804 60758EBC 60753AB4 60753E24 60754BC4
```

CSCee26884

When the permanent virtual path (PVP) was changed while a large number of VCs (more than 100 VC) were in the tunnel and traffic was running, ATM segmentation and reassembly (SAR) generated an error message and, under extreme conditions, the line card failed. The Cisco IOS software did not manage the error message as expected and sometimes also failed. This has been fixed.

CSCee29154

Sometimes access control lists (ACLs) were not applied to virtual access interfaces. This has been fixed.

CSCee32235

The multilink state machine was not operating properly because it was being indexed by the multilink queue index instead of the preferred static bundle index. The multilink queue index changed each time the bundle first in first out (FIFO) buffer was replaced. This has been fixed.

CSCee34998

When a multilink PPP (MLP) bundle shut down due to the loss of its peer or because it was manually shut down, draining of the bundle FIFO sometimes was delayed for up to 30 minutes due to new packets traveling into the default queue of the member's serial interface. This condition caused an unacceptable delay in bringing the bundle back up after disabling it. When you entered the **show pxf cpu queue multilink<n>** command during this condition, the Packets in Bundle FIFO field displayed a non-zero value. This has been fixed.

CSCee35033

When running the Cisco IOS experimental image c10k2-p11-mz.v122_16_bx_throttle.20040416, a Cisco 10000 router sometimes encountered a bus error failure. This has been fixed.

CSCee35665

When a nested service policy was applied to a Gigabit Ethernet subinterface with a terminated PPPoE over VLAN session, any traffic that matched the service policy was not forwarded to the PPPoE over VLAN session. This has been fixed.

CSCee37568

When using SNMP with the CISCO-CLASS-BASED-QOS-MIB for a class-default class configured with random-detect, the cbQosREDClassStatsTable did not have an entry for class-default. This has been fixed.

CSCee39928

The priority queue (PQ) counters were not working with link fragmentation and interleaving (LFI). When you entered the **show policy-map** command, the PQ counters were not working and remained zero (0). The drop counters for SNMP were zero (0) for all queues. This has been fixed.

CSCee44158

The multilink PPP (MLP) minimum fragment size was incorrect. The minimum fragment size set was 66 instead of 56 (64 bytes minus 8 bytes header). This has been fixed.

CSCee45388

Multicast packets received on a PPPoE interface and sent out a GRE tunnel were not encapsulated correctly. The remote end of the GRE tunnel dropped the packet as an unknown type packet. This has been fixed.

CSCee48311

When the SSG host object connected to two or more services, a system processor memory leak occurred in the SSGSerQue process. This has been fixed.

CSCin66679

When an unauthenticated user tried to access a service, the TCP packets for the host were redirected to the SESM, but the returned packets were not reverse translated. This occurred on the Cisco 10000 router with PXF switching when the SSG TCP Redirect feature was enabled for unauthenticated users and the SSG Port Map feature was disabled. This has been fixed.

CSCin68702

SSG service binding to the next-hop gateways failed when the configuration of the router was copied to the router from the TFTP server. This caused SSG services to sometimes become inaccessible. 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. See the [“Obtaining Technical Assistance” section on page 28](#).

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.

CSCea66654

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 **no ip access acl-name** command. This occurs if the interface is rechannelized and the removed ACL is reconfigured on the interface. 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.

CSCeb77168

If two users were logged into the router, and one user began a save of the system configuration to removable flash media while another user initiated a system reload, the configuration file on the removable media became corrupted and no file operations were possible on the file (for example, erase, copy, and overwrite did not work). We have been unable to reproduce this problem.

CSCeb77178

If you wanted to store a configuration locally on removable flash media disk0 and you were using the boot config statement and the boot config environment variable to point to the same configuration file on disk0, the file was not automatically synchronized to disk0 on the redundant PRE (sec-disk0). In the event of a failure, the backup PRE would not have had access to the current configuration file. We have been unable to reproduce this problem.

Related Documentation

The following documents are specific to Cisco IOS Release 12.2(16)BX3:

- [Variable Bit Rate-Non-Real Time Oversubscription, Release 12.2\(16\)BX3 feature module](#)
- [SSG Link Redundancy, Release 12.2\(16\)BX3 feature module](#)
- [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

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

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

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.

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

- 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

- 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.