



Release Notes for the Cisco 10000 Series Router for Cisco IOS Release 12.3(7)XI3

First Published: March 17, 2005

Revised: January 24, 2007

OL-5057-04

These release notes provide information about Cisco IOS Release 12.3(7)XI3, which provides broadband aggregation, leased-line, and MPLS features for the Cisco 10000 series router.

For a list of the software caveats that apply to Cisco IOS Release 12.3(7)XI3, see the “[Caveats for Cisco IOS Release 12.3\(7\) XI3](#)” section on page 9 and *Caveats for Cisco IOS Release 12.3 T*. The caveats document is updated for every maintenance release and is located on [Cisco.com](#).

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

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. 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.htm

Cisco IOS Release 12.3(7)XI3 is based on the following releases:

- Cisco IOS Release 12.2(16)BX
- Cisco IOS Release 12.3T
- Cisco IOS Release 12.3(7)XI3

To review the release notes for Cisco IOS Release 12.2(16)BX, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10krn/122bx/index.htm>

To review the release notes for Cisco IOS Release 12.3, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/xprn123/index.htm>



Corporate Headquarters:

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

© 2005 Cisco Systems, Inc. All rights reserved.

Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [New Features—Cisco IOS Release 12.3\(7\)XI3, page 3](#)
- [Limitations and Restrictions, page 4](#)
- [Important Notes, page 6](#)
- [Caveats for Cisco IOS Release 12.3\(7\) XI3, page 9](#)
- [Obtaining Documentation, page 57](#)
- [Documentation Feedback, page 58](#)
- [Cisco Product Security Overview, page 58](#)
- [Obtaining Technical Assistance, page 59](#)
- [Obtaining Additional Publications and Information, page 61](#)

System Requirements

Cisco IOS Release 12.3(7)XI3 requires that you have the performance routing engine (PRE), Part Number ESR-PRE2 installed in the Cisco 10000 series router chassis. To verify which PRE is installed in the router, use the **show version** command.

Route Processor Redundancy Mode

The Cisco 10000 series router supports route processor redundancy (RPR) mode or RPR+ mode to provide fault resistance and to ensure high availability. In RPR mode, one supervisor engine is active and operational while the second supervisor engine is in standby mode waiting for the active supervisor to fail so that it can take over and maintain the operation of the router. In RPR+ mode, the standby supervisor engine is fully initialized and configured, which shortens the time needed to switch over to the standby supervisor.

When upgrading or downgrading the Cisco IOS software, the RPR mode used on the Cisco 10000 series router depends upon the Cisco IOS software currently running on the Cisco 10000 series router and the Cisco IOS software to which you want to upgrade or downgrade.

Table 1 lists the RPR modes used when upgrading or downgrading Cisco IOS software. For example, when upgrading to Cisco IOS Release 12.3(7)XI3 from Release 12.2(16)BX, the router uses RPR mode instead of RPR+ mode. When downgrading to Cisco IOS Release 12.2(16)BX from Cisco IOS Release 12.3(7)XI3, the router uses RPR mode.

Table 1 RPR Modes for Cisco IOS Software Releases

Releases	12.2(16)BX	Cisco IOS Release 12.3(7)XI3
12.2(16)BX	RPR+	RPR
12.3(7)XI3	RPR	RPR+

Before You Upgrade the Cisco IOS Software

Before you upgrade (or downgrade) the Cisco IOS software running on the Cisco 10000 series router, save the running configuration file. In RPR mode, the router synchronizes only the startup configuration.

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 Router Line Card 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 12.3(7)XI3

The following new features and improvements are supported on the Cisco 10000 series router in Cisco IOS Release 12.3(7)XI3.

- [PPPoE Circuit-ID Tag Processing, page 3](#)
- [QoS: Broadband Aggregation Enhancements - Phase 1 \(LAC QoS\), page 4](#)

For more information about the new features in Cisco IOS Release 12.3(7)XI3, refer to the following documentations:

- [Cisco 10000 Series Router Broadband, Leased-Line, and MPLS Configuration Guide](#)
- [Cisco 10000 Series Router QoS Configuration Guide](#)

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

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

PPPoE Circuit-ID Tag Processing

The PPPoE Circuit-ID Tag Processing feature enables Ethernet-based access network services by providing a mechanism for a PPPoE Broadband Remote Access Server (BRAS) to map a subscriber's circuit ID (that is, the line ID) to a specific Ethernet interface.

A Digital Subscriber Line Multiplexer (DSLAM) can be configured to insert a unique circuit-ID tag into a PPPoE Active Discovery Initiation/PPPoE Active Discovery Request (PADI/PADR) frame. You can create a PPPoE profile to enable the PPPoE BRAS to process the vendor tag to send the circuit-ID portion of the tag (as NAS-Port-ID attribute 87) to the RADIUS server in all authentication, authorization, and accounting (AAA) access and accounting requests. You can also create a PPPoE profile to strip the vendor tag from outgoing PPPoE Active Discovery Offer (PADO) and PPPoE Active Discovery Session (PADS) frames.

For more information, see the *PPPoE Circuit-ID Tag Processing* documentation at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftpprfls.htm>

QoS: Broadband Aggregation Enhancements - Phase 1 (LAC QoS)

The QoS: Broadband Aggregation Enhancements - Phase 1 (LAC QoS) feature enables you to attach a QoS service policy to an ATM VC on the LAC using the **service-policy** command. The sessions that use the ATM VC inherit the service policy attached to the VC or the inherited policy of the VC. If a session inherits a policy, the **show policy interface virtual access** command does not display the state of the inherited policy. You can display the state of the policy only on the interface where you configured the policy.

For more information, see “Chapter 4, Attaching Service Policies” in the *Cisco 10000 Series Router Quality of Service Configuration Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/qoscf/index.htm>

Limitations and Restrictions

This section describes limitations and restrictions for the following areas. Be sure to review the following limitations and restrictions before using the features in Cisco IOS Release 12.3(7)X13:

- [Controlling the Rate of Logging Messages, page 4](#)
- [Frame Relay, page 4](#)
- [PRE Network Management Ethernet Port, page 5](#)
- [Scalability, page 5](#)
- [Testing Performance of High-Speed Interfaces, page 5](#)

For more information about the restrictions for a specific feature, refer to the *Cisco 10000 Series Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*.

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.

Cisco recommends that you configure the **logging rate-limit** command as follows. This limits the rate of all messages to the console to 10 per second, except for messages with critical priority (level 3) or greater.

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

For more information, refer to the **logging rate-limit command** in the *Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3*.

Frame Relay

The following limitations apply to the Cisco 10000 series router implementation of Frame Relay:

- The **ip rtp reserve** command is not supported.
- Only one priority queue per VC is allowed.

PRE Network Management Ethernet Port

Ensure that the Fast Ethernet NME port on the PRE is configured for auto-negotiation mode, which is the system default. Duplex mode can cause problems, such as flapping. If the port is experiencing such problems and has been configured for duplex mode, use the **no half-duplex** or **no full-duplex** command to disable duplex mode.

Scalability

If you configure create on demand PVCs (individual and within a range) and PPP sessions, RP CPU utilization can be extremely high when bringing up and tearing down sessions and PVCs. This is only a concern when the configuration contains approximately 30,000 PPP sessions, and additional services are enabled such as DBS, ACLs, and service policies.

To reduce the RP CPU usage for PPPoA sessions, reduce the number of configured PVCs in a single subinterface. To reduce the RP CPU usage for PPPoEoA sessions, use call admission control (**call admission limit** command).



Note

Do not configure more than 1500 VCs under a multipoint interface. Exceeding this recommended limit can cause very high CPU utilization. Refer to CSCeh07013 in [Resolved Caveats—Cisco IOS Release 12.3\(7\)XI3, page 35](#).

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 for 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 may 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 hardware pxf cpu queue** command.

Important Notes

This section provides important information about the following topics:

- [Configuring the `aaa new-model` Command](#), page 6
- [Enhancing Scalability of Per-User Configurations](#), page 6
- [Inserting a New Line Card](#), page 8
- [Local AAA Server, User Database—Domain to VRF](#), page 8
- [Provisioning for Scaling](#), page 8

Configuring the `aaa new-model` Command

The `aaa new-model` command is disabled by default on the Cisco 10000 series router. In previous releases, the default configuration did not appear in the running configuration file. However, in Cisco IOS Release 12.3(7)XI1 or later releases, the running configuration file now includes the `no aaa new-model` command. This is an intentional change in behavior for this command and is the first step in a three-step process to change the default configuration to `aaa new-model`.



Note

This change in behavior differs from Cisco IOS software, which typically does not include default configurations in the running configuration file.

For example, when you enter the `show running-config` command, `no aaa new-model` appears in the configuration if either of the following conditions previously occurred:

- You did not configure the `aaa new-model` command on the router and instead accepted the default configuration of the file: `no aaa new-model`.
- You entered the `no aaa new-model` command to remove the previously configured `aaa new-model` command.

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 VRFs and IP unnumbered interfaces. The VSAs apply to virtual access subinterfaces and are processed during PPP authorization.

In releases earlier than 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 series 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 series 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"
```

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

Whenever you specify a VRF in a user profile, but you do not configure the VRF on the Cisco 10000 series 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 series 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 series router attempts to apply a large number of per-user profiles that include the **lcp:interface-config** VSA. Therefore, when updating your user profiles, we recommend that you redefine the **lcp:interface-config** VSA to the scalable **ip:vrf-id** and **ip:ip-unnumbered** VSAs.

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

Example 1 Redefining VRF Configurations

Change:

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

To:

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

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

Example 2 *Redefining IP Unnumbered Interfaces*

Change:

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

To:

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

Inserting a New Line Card

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

Local AAA Server, User Database—Domain to VRF

Local AAA Server, User Database—Domain to VRF is working correctly in Cisco IOS Release 12.3(7)XI3. (It was not working correctly in Cisco IOS Release 12.3(7)XI2).

Provisioning for Scaling

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

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

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

For more information, refer to the *Cisco 10000 Series Broadband Aggregation and Leased-Line 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
```

Caveats for Cisco IOS Release 12.3(7) XI3

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

This section contains open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T that apply to the Cisco 10000 series are also in Cisco IOS Release 12.3(7)XI3.

For information on caveats in Cisco IOS Release 12.3, see *Caveats for Cisco IOS Release 12.3*.

For information on caveats in Cisco IOS Release 12.3 T, see *Caveats for Cisco IOS Release 12.3 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on [Cisco.com](http://www.cisco.com).



Note

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](http://www.cisco.com) and click **Products and Services: Cisco IOS Software: Cisco IOS Software Releases 12.2: Troubleshooting: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

Open Caveats—Cisco IOS Release 12.3(7)XI3

This section describes caveats that are open in Cisco IOS Release 12.3(7)XI3.

- CSCdt94857

High impact commands or commands used in high scaling environments impact scaling by increasing CPU cycles, increasing boot time, and decreasing control plane run-time efficiency.

There are no known workarounds.

- CSCdy45049

When scaling over 3000 serial interfaces, line rate traffic may not be achieved. This problem occurs when thousands of serial interfaces (PPP or HDLC) are used on the port and line rate traffic is sent through all interfaces.

There are no known workarounds.

- CSCdz40002
When you remove APS and then re-activate it, traffic convergence after an APS switchover takes longer than 2 seconds.
There are no known workarounds.
- CSCea63115
When you enter the **redundancy force-failover main-cpu** privileged EXEC command on a router that is configured with two Performance Routing Engines (PREs), an automatic protection system (APS) switchover occurs on OC-12 Packet-over-SONET (POS) line cards, which is incorrect behavior.
This problem occurs when APS is configured on OC-12 POS line cards in two different Cisco 10000 series routers that are connected back-to-back and you enter the following sequence of commands:
 1. Enter the **aps force pos slot/subslot/port from working** interface configuration command on both routers.
 2. Enter the **show aps** EXEC command. The output displays the active channels for both routers.
 3. Enter the **redundancy force-failover main-cpu** privileged EXEC command on one of the routers, causing an APS switchover to occur on this router.
 There are no known workarounds. However, when problem occurs, there is no loss of data.
- CSCea63638
When Automatic Protection Switching (APS) is enabled, if you issue the **hw-module reset** command on the primary APS slot, no change is observed because the router does not switch to the secondary APS slot. This problem occurs when the **hw-module reset** command is issued.
There are no known workarounds.
- CSCec13372
The router can generate wrong or misleading sub-pool or global pool flooding messages when up or down thresholds for MPLS TE resource availability (bandwidth) are crossed. The configured thresholds for MPLS TE resource availability are crossed when defining bandwidth on the MPLS tunnel interface reserved on the physical interface/subinterface.
There are no known workarounds.
- CSCec37207
On Cisco 10000 series routers running in PTA mode, PPPoEoA sessions using bandwidth queues drop packets if a priority queue is also configured in the policy map. When there is traffic sent to priority queue, all other queues can drop packets below line rate if the traffic consists of small packets.
There are no known workarounds.
- CSCec42315
When scaling to 12,000 Frame Relay DLCI interfaces, line rate traffic may not be achieved. This problem occurs when thousands of Frame Relay DLCIs are used on the port and line rate traffic is sent through all interfaces.
There are no known workarounds.
- CSCec42451
The RIP routing protocol does not function properly over VLAN interfaces with IP unnumbered.
There are no known workarounds.

- CSCec43937

When you run hierarchical shaping, a small number of UPC violations can occur on a DS3 ATM interface on an LS1010 that is connected to a LAC. The traffic shaped by the LAC is slightly above the tunnel PCR. The number of violations does not depend on the tunnel oversubscription but seems to be proportional to the tunnel PCR.

There are no known workarounds.
- CSCec48111

When sending 64 byte packets through 300 serial interfaces or more, line rate traffic may not be achieved. This problem occurs with 64 byte packets and a large number of interfaces.

There are no known workarounds.
- CSCec80927

Call setup rate slower is for a particular configuration running on a 12.3(6)TX image compared with 12.2(16)BX. If the **mtu** command is added to the vtemplate for sessions, the command processing for the command takes significantly longer on a 12.3(6)TX image as compared to a 12.3(16)BX image.

Workaround: Remove the **mtu** command from the vtemplate configuration.
- CSCec85628

Outgoing traffic is above VP speed on an 8e3d3atm line card. For this problem to occur, the total SCR value of all VBR-nrt VCs in a VP is above 80 percent of the VPs PCR value but still smaller than the total VP bandwidth (PCR). All the VCs should be overdriven by outgoing traffic.

There are no known workarounds.
- CSCed03248

The CLI error “IP address is already defined as an interface” appears when the address is not used anywhere in the running configuration. The error occurs when the IP address was used by a serial interface and the interface was removed or unconfigured from the system.

Workaround: Use the **no ip address** command before removing a serial interface or use a different IP address (if possible).
- CSCed17570

When using thousands of QoS queues with WRED configured in each queue, a traceback message can appear when you execute the **microcode reload pxf** command. The traceback message appears only when thousands of PXF queues are configured with random-detect enabled and the **microcode reload pxf** command is issued.

There are no known workarounds.
- CSCed20626

‘Exec’ process CPUHOG occurs. This is caused by the **dir all** command, probably due to the attempted accesses to the secondary's PCMCIA slots.

There are no known workarounds. The router continues to function, but the console is unusable for a short while(10-30 seconds). Alternatively, use the **dir device** commands only for known good device names.
- CSCed29494

The maximum queue limit for a low -speed link is 4,096, but the system allows you to set the queue limit to 8192.

There are no known workarounds.

- CSCed54867

The input service policy does not match traffic as shown by the **show policy-map interface** command if there is no action associated for that class.

Workaround: Set up an action such as “set” or “police”.

- CSCed59185

When you apply the following example configuration to an output interface that is MPLS enabled, and send traffic from the CPU of the local router (ping other routers or hosts), the traffic is not policed by the policy map.

```
Policy Map exp2cos
Class exp0
set cos 1
Class exp1
police 104000 5000 150800 conform-action transmit exceed-action drop violate-action
drop
Class exp2
```

This problem only affects the traffic from the router CPU, and does not affect traffic passing through the router.

There are no known workarounds.

- CSCed62503

When you apply a policy map to a tunnel interface on a router configured with a PRE2 processor, a traceback message appears. This problem occurs when the policy map is applied to a tunnel interface.

There are no known workarounds.

- CSCed65349

When you configure 2,000 PPP interfaces, traffic does not reach 99 percent of the line rate after performing 4 HA RPR switchovers. The traffic rates keep fluctuating.

There are no known workarounds.

- CSCed68868

A traceback message appears when you unconfigure the spoke PE router configured for half-duplex VRF over PPPoE. This problem occurs with 32,000 PPPoE sessions and 40 spoke VRF, therefore scaling to high values.

There are no known workarounds.

- CSCed70202

A traceback message appears when you unconfigure the hub PE router configured for half-duplex VRF. This problem occurs with 32,000 sessions, therefore scaling to high values.

There are no known workarounds.

- CSCed71107

When 2 time-based ACLs are configured to deny traffic at the same time and are applied to different interfaces, one of the ACLs fails to work properly.

There are no known workarounds.

- CSCed72023
Excessive CPU utilization is detected for 5 minutes after unconfiguring half-duplex VRF with a large number of PPPoE user sessions. This problem occurs with 32,000 PPPoE sessions, therefore scaling to high values.
There are no known workarounds.
- CSCed72338
The system allows non-nested queuing policy maps to be applied via the **frame-relay map-class** command on Frame Relay main interfaces and subinterfaces; it should not allow such policy maps to be configured.
There are no known workarounds.
- CSCed86371
The Automation Protection Switching (APS) active state does not stay with the lowest active odd port after a PRE switchover.
There are no known workarounds.
- CSCed88782
The secondary port does not go to a working state during a signal degrade of the primary port using threshold SON ERR RAT 1e-6.
Workaround: Set the BIP threshold to 6; do not set the BIP threshold to 7.
- CSCee02536
When configuring MPLS Layer 3 VPN, the PXF CEF/FIB table can hold up to 4,085 VRFs, although it is designed to hold 4,095 VRFs. If more than 4,085 VRFs are configured, 10 of those VRFs do not have an entry in the PXF CEF/FIB table, so traffic is not forwarded in those 10 VRFs.
There are no known workarounds.
- CSCee03801
After you issue the **clear ip bgp *** command, a Cisco 10000 series router takes longer than 30 minutes to achieve convergence. eBGP sessions between PE and CE routers can go up and down multiple times, and the IGP routing protocol and LDP session can also go down and up again.
These problems occur under the following conditions:
 1. 4,095 VRFs are configured on a router
 2. 500 eBGP sessions are established between the router (PE) and CE routers
 3. 540 VRF routes per VRF in the 500 VRFs that are running eBGP between PE and CE routers
 4. 40 VRF routes per VRF in the rest of 3595 VRF
 There are no known workarounds.
- CSCee06089
When you apply a nested policy map using the **bandwidth** command in the child policy map to a POS OC48 interface, PXF stops responding. This problem occurs when you allocate a small amount of bandwidth, and it only occurs on POS OC48 interfaces.
Workaround: Allocate more bandwidth in the child policy map.

- CSCee14864
Policing under a created queue, when attached at an MLP interface, accounts for only 2 bytes of the L2 header, so that policing is done at a higher rate than configured. This can cause a problem with priority queue CBWFQ functionality because the priority queue is configured with policing and its dequeue rate can be higher than intended.
Workaround: Do not configure policing under a created queue.
- CSCee15674
When broadband PTA is configured with 114,000 queues, executing the **microcode reload pxf** command causes the ATM interface to display a big number of total output drops.
Workaround: Clear the counters.
- CSCee20418
If the you change the amount of intercepted streams from 8 to 2 streams, the wrong amount of packets is intercepted. This occurs in Lawful Interception scenarios.
There are no known workarounds.
- CSCee25615
This problem occurs when almost all the system resources (VCCI) are in use, after an OIR (slot reset) is issued, and in the OC3 ATM line card. The reason it occurs in the OC3 ATM line card is that it happens in an ATM line card with multiple ports. The symptom is that all the sessions in the same port stop passing traffic after OIR.
There are no known workarounds.
- CSCee27630
A low-bandwidth class can be allocated more than its share of bandwidth at the expense of a high-bandwidth class. This problem occurs when the ratio of the configured bandwidths between two data classes is high (8:1 or higher) and when there is a priority class that receives traffic at (at least) 20 percent of the line rate. The traffic that is received by the data classes should be in the ratio of the configured bandwidths.
There are no known workarounds.
- CSCee42746
When using multiple intercepts in Lawful Intercept mode, the MIB information is not completely cleared after intercepts are cleared from SNMP. This problem occurs when 35 or more streams are intercepted at the same time.
Workaround: Use Cisco IOS to delete the stream that was not deleted by SNMP.
- CSCee44273
The **show activity** line card debug command shows the VC configuration from the perspective of the line card, but the autovc information is not shown. Also, after you delete or create an autovc, the counter is inaccurate.
There are no known workarounds.
- CSCee45306
With 40 or more intercept streams in Lawful Intercept mode, the LI engine fails to intercept correctly for UDP traffic. This problem occurs when 40 or more streams are intercepted at the same time.
There are no known workarounds.

- CSCee45378

When intercepting streams at 5 Mbps or above in Lawful Intercept, the router CPU runs at about 78 percent of capacity. This problem occurs when 35 or more streams are intercepted at the same time. There are no known workarounds.
- CSCee50060

A Cisco 10000 series router with PPPoA VCs can, under abnormal conditions (such as a denial-of-service attack involving the sending of PPPoA data packets before the PPPoA session is up), experience heavy RP CPU use. The router with PPPoA VCs can forward PPPoA data packets for non-existent sessions.

This problem occurs when PPPoA data traffic is sent before the session reaches the PTA forwarded state. A normal PPPoA client does not send traffic before the session is up.

Workaround: Configure RPF on all ATM subinterfaces containing PPPoA sessions. The subinterface should have an RPF check in addition to using an RPF check in the virtual template. Configuring RPF on the subinterface forces all PPPoA data traffic to be dropped by the PXF before the session reaches the PTA forward state.
- CSCee54408

When the 1choc12 line card uses SDH framing, the Path Trace Buffer is unstable for au3 mode. This problem occurs only with SDH framing; the Path Trace Buffer is stable with SONET framing. There are no known workarounds.
- CSCee54426

When the 1choc12 line card uses SDH framing, the J1 Path trace message is not received. This problem occurs only with SDH framing. The J1 Path Trace message is received when SONET framing is used. There are no known workarounds.
- CSCee54473

A loss of frame (LOF) alarm appears for a T1 when framing SF is configured on both ends. This problem occurs when you configure **T1 1 framing sf** under AU-3 on a 1 port channelized OC12 line card. There are no known workarounds.
- CSCee54971

The **show policy-map interface** command output does not display the layer 2 frame size correctly. The actual output policing rate is 6.6 percent higher than the configured policing rate on gigabit Ethernet and POS OC48 interfaces. The problem occurs when a **police** command is configured in a policy map, and the policy map is applied to a gigabit Ethernet or POS OC48 interface as an output policy map.

Workaround: Use shaping instead of policing.
- CSCee55828

You cannot configure **t1 1 framing esf** and **t1 loopback remote** at the same time on a 1-port channelized OC12 line card. This problem occurs when you configure **t1 1 framing esf** under an AU-4 on a 1-port channelized OC12 line card.

Workaround: Configure **t1 1 framing esf** without the loopback configured for the T1.

- CSCee57219

The **set cos** command in an output policy map applied to a VLAN subinterface does not work if the outgoing traffic is MPLS packets (with MPLS labels). The problem occurs when outgoing traffic is MPLS packets.

There are no known workarounds.
- CSCee57357

When scaling Frame Relay DLCIs on routers running IOS version 12.3(7)XI, traceback messages can appear on the console when bringing up the high number of DLCIs. This problem occurs when there are more than 3,000 DLCIs on the interface.

There are no known workarounds.
- CSCee58454

On a router running 12.3(7)XI, if the LAC tries to redirect a call to the bid-winning LNS and fails after three attempts, a new RADIUS disconnect cause code with the value as 608 is not being sent to RADIUS by the LAC.

There are no known workarounds.
- CSCee60038

When a proxy service profile defined with V & X attributes is configured locally on the router, which is enabled to run SSG, an SSG host cannot activate the service it has been subscribed to.

There are no known workarounds.
- CSCee60101

ALIGN-3 traceback messages are displayed while running regression tests on a channelized OC12 line card with sonet 768 encap with E1 framing. This problem does not seem to affect the functionality of the card.

There are no known workarounds.
- CSCee61067

In 2-level policy map configurations using a parent shaper, the shaped traffic rate might not be within plus or minus 1 percent of the configured value. This problem occurs with certain parent shaper values and mostly small packet sizes.

There are no known workarounds.
- CSCee61485

Several PIM-related messages appear on the console when you remove, then re-apply a PIM configuration on the interface. This problem occurs when the removal and re-application of the configuration is done in a rapid manner.

There are no known workarounds.
- CSCee61502

When configuring an MLPPP interface on a redundant system, the standby PRE adds the **no ip route-cache cef** interface command to multilink interfaces. This additional line causes the system to generate the following error when the new standby PRE is reloaded:

```
May 19 13:20:47.222 EDT: %REDUNDANCY-3-CONFIG_SYNC: Active and Standby bulk configuration out of sync
```

Workaround: Remove the **no ip route-cache cef** command from each multilink interface.

- CSCee62159
Actual output and expected output for packet 1 does not match at nibble 8. This packet (packet_no 1, fragment_no : 1) is received in the wrong order. Other packets are also received in the wrong order. This problem occurs with the bootflash:c10k2-p11-mz.v123_7_xi_throttle.040510 image and the test is passed with Feb17 bba image.
There are no known workarounds.
- CSCee63636
MPLS:Traceroute does not show Labels being switched-propagate-ttl ON.
There are no known workarounds.
- CSCee64067
Traffic is not forwarded to an RBE client in a VRF. This problem occurs when an RBE client that doesn't respond to ARP requests, exists in a MPLS VPN. A static ARP entry for the client must be configured on the access router but the traffic is still not forwarded due to this problem
There are no known workarounds.
- CSCee65789
A 4 percent packet drop is seen for various packet sizes over a 1choc12-sdh interface when running performance/scalability tests.
There are no known workarounds.
- CSCee66066
BERT testing over a clear channel DS3 interface for the 1CHOC12 line card fails as a result of the DS3 interface, which remains in a DOWN state.
There are no known workarounds.
- CSCee66091
During SNMP polling of the AAA Server MIB, the casDeadCount variable can cause a CPU hog on the router. This problem occurs with a large number of RBE interfaces (16,000) and bi-directional traffic running.
There are no known workarounds.
- CSCee66314
In Lawful Intercept mode a traceback message might appear on the Intercept Access Point (IAP) router when the interface to the mediation router is shut down. This problem occurs when traffic is sent through the IAP and interception is turned on.
There are no known workarounds.
- CSCee68404
If a PRE2 is in the early process of booting up, sometimes the SEND-BREAK character sequence can cause the router to reload instead of gracefully dropping back into ROMMON. This problem occurs when the PRE2 is in the early stages of the boot process and the SEND-BREAK is issued. If the PRE2 is already booted up, this is not an issue.
Workaround: To gracefully drop the PRE2 into ROMMON, if the configuration register is set to accept SEND-BREAK, wait until the PRE2 is fully booted.

- CSCee68480

Priority queue latency can exceed the threshold of 2MTU+6msec. This problem occurs when more than 3 queues are configured on a interface, in addition to the priority queue.

There are no known workarounds.
- CSCee72919

AAA accounting records for a PPPoA session terminated on a Cisco 10000 series router in a PTA fashion shows repeated entries for the Framed-Route attribute (attribute 22).

There are no known workarounds.
- CSCee72931

When a PPPoA session is cleared on the PTA router using the **clear pppatm interface ATM X/Y/Z.A** command or the **clear int virtual-access** command, the accounting stop record does not display the Octet and Packet counters. This problem occurs only when the session is cleared on the PTA router. If the user disconnects the session, the counters are displayed correctly.

There are no known workarounds.
- CSCee81270

When a source sends packets to a destination under the TCP protocol, the destination sends an echo response back to the sender. With the intercepting router configured to intercept "all", those echo packets should also be picked off. This does not occur.

There are no known workarounds.
- CSCee86091

The show version command does not display the bootloader image name.

Workaround: There is no workaround for this problem.

CSCee90904In the presence of a large number of static routes (16,000- 32,000), line card flap/router reload/OIR cause high CPU usage for a long period of time.

There are no known workarounds.
- CSCee93055

When clearing a PPPoE session using the **clear pppoe all** or **clear interface virtual-access x.y** command, the router displays the following messages:

```
XCM access error at ../toaster/c10k_rp/c10kds2_qos.c (4888) Jun 23 12:34:12.587:
c10k_ttcmm_read: Invalid Address 3FC110A4
```

This problem occurs when the ATM interface VC is configured with **protocol pppoe** and **dbns enable** (Dynamic Bandwidth Selection).

There are no known workarounds.
- CSCee94457

Actual throughput is lower than expected throughput (94 percent of expected throughput). This problem occurs when testing CAR (with MQC Policy command) on 4 Port OC3 ATM line card, packet size is 64 bytes, and encapsulation type is aal5snap. There is no problem with a packet size of 128 bytes or higher. If the encapsulation type is aal5mux, no problem is found.

There are no known workarounds.

- CSCee95619

Attribute 1 User-Name is not included in Stop records from LNS. This problem occurs when the LNS router runs the 12.3(5a)B image.

There are no known workarounds.
- CSCee96582

With broadband multipoint 31,500 PVCs with 30,000 sessions up, 126,000 queues, and you add a class with the **set** command in an output policy map on the fly, the router hangs for a long time then crashes. This problem occurs with broadband multipoint PVCs with 30,000 sessions up, 120,000 queues, then you add a class with the **set** command in a policy map on the fly.

There are no known workarounds. With a large number of sessions and queue scaling, avoid changing policy map on the fly.
- CSCef00808

The **show pxf cpu stat security** command shows incorrect statistics when Legal Intercept is configured along with time-based or regular access lists. This problem occurs only if Legal Intercept and access lists are configured and are interoperating

There are no known workarounds.
- CSCef05454

In a router running Cisco IOS Release 12.3(9), the PPPoA sessions can get stuck in LCP_NEGOTIATION. The problem also occurs in Cisco IOS Release 12.2T. The output of the **show atm pvc** command shows the number of packet and cell drops incrementing continuously:

```
InPktDrops: 0, OutPktDrops: 13376/0/13376 (holdq/outputq/total) InCellDrops: 0,
OutCellDrops: 12178
InByteDrops: 0, OutByteDrops: 198692
```

The status of the sessions cycles between the following states and gets stuck in LCP_NEGOTIATION:

```
Jul 1 12:41:54.187: PPPATM: ATM2/0.1 1/176 [1220], State = WAIT_FOR_CALL
Jul 1 12:41:55.139: PPPATM: ATM2/0.1 1/176 [1220], State = INCOMING_CALL
Jul 1 12:41:55.139: PPPATM: ATM2/0.1 1/176 [1220], State = NAS_PORT_POLICY_INQUIRY
Jul 1 12:41:55.139: PPPATM: ATM2/0.1 1/176 [1220], State = PPP_START
Jul 1 12:41:55.139: PPPATM: ATM2/0.1 1/176 [1220], State = LCP_NEGOTIATION
```

Workaround: Reload the router.
- CSCef08967

The WRED sampling frequency is too slow, which can cause jitter for the overall algorithm.

There are no known workarounds.
- CSCef09119

With broadband PTA 128,000 queue with input and output policy map, removing the input policy from Virtual-Template causes a CPUHOG traceback message. This occurs when configuring 31,500 ATM subinterfaces with output CBWFQ policy, and input police policy in Virtual-Template, bringing up 30,000 PPPoE sessions, and removing the input policy map.

There are no known workarounds.
- CSCef14249

When sending traffic with 1,024 byte large size packets over 120,000 queues with 80 percent oc12atm line rate, traffic drops 10 percent due to buffer_low packet drop. This problem occurs when 120,000 queue scaling is configured with only large packet size traffic.

There are no known workarounds. Send traffic with mixed size packets, tending to small packets.

- CSCef15141
On Cisco 10000 series routers running Cisco IOS Release 12.3(7)XI, the Priority Queue latency values (in milliseconds) is higher than $2 * MTU + 6ms$ on 4Mbps and 8Mbps subrates of the 8e3ds3 line card.
There are no known workarounds.
- CSCef17801
When configuring over 2,000 Frame-Relay DLCI interfaces on a 1choc12 line card, the router's CPU runs over 30 percent of its capacity. This problem occurs only if the number of Frame-Relay sub-interfaces is over 2,000.
There are no known workarounds.
- CSCef18947
The **show vlans** command does not report the correct statistics when a second CPU is enabled on 7301/NPPEG1 platforms.
Workaround: Disable the second CPU, however, this affects performance.
- CSCef19259
If autovc is configured, tracebacks can occur when an ATM VC is deactivated.
There are no known workarounds.
- CSCef20523
PPPoEoA sessions using CBWFQ experience BQ drops. In some cases, when aggregate traffic is near the VC rate, the BQ tail drops packets. This problem appears with low bandwidth VCs, in this case 196 kbps.
Workaround: Changing the queue-limit via the policy map and/or the VC queue depth will improve the result.
- CSCef24008
When using a 4choc3 line card and 300 or more VT T1 interfaces are configured with PPP encapsulation, some T1 links do not achieve full traffic line rate. This problem occurs when all 300+ interfaces are sending traffic at line rate concurrently.
There are no known workarounds.
- CSCef24551
When running Automated Protection Switching (APS), the router can experience traffic loss after the **hw-module slot x reset** command is executed.
Workaround: Avoid executing **hw-module slot x reset**.
- CSCef27202
On Cisco 10000 series routers running in PTA mode, a CPU hog message appears if you execute the **show vpdn session** command when there are more than 30,000 sessions active. This problem occurs if the number of active sessions is large.
There are no known workarounds.
- CSCef27221
When a router runs as a LAC and the rate at which PPPoA sessions are established is high, some sessions may not be established and the router can display an error message on the console. This problem occurs when 30,000 PPPoA sessions or more are established at high rate, such as when the ATM link to the DSLAM is restored after a link failure.

Workaround: Reduce the call admission rate for the PPPoA sessions.

- CSCef27417

Output drops can be erroneously reported on the ATM OC12 interface upon reloading the router and without any traffic sent or received on the interface. The output drops interface counter may also report invalid non-zero values with a light traffic load on the interface (PPPoX session establishment). This problem occurs when a high number of VCs is configured on the interface.

There are no known workarounds.

- CSCef27539

PPPoEoA sessions experience priority traffic drops when using an absolute priority configuration. This problem occurs during traffic congestion; with 8,000 PPPoEoA sessions, priority traffic is dropped at the line card.

Workaround: Modifying the VC queue depth improves but does not alleviate the drops. Changing the configuration to a generic PQ configuration (without absolute priority) alleviates the drops.

- CSCef30736

When using WRED with 10,000 queues on 4,000 ATM subinterfaces after counters have been cleared, the total output drops on the ATM interface increases without any traffic.

Workaround: There is no workaround for this problem.

- CSCef30873

The router can crash due to an "Unexpected Exception" when you flap several Multilink PPP interfaces several times. This problem occurs when over 50 MLPPP interfaces are concurrently brought up, then down, several times in a short period of time.

There are no known workarounds.

- CSCef31662

The first serial interface on a line card is down after adding it to an MLP bundle. This problem occurs when the interface had been configured earlier as a bundle member, removed together with the bundle and then created back again.

There are no known workarounds.

- CSCef32203

A serial interface using PPP encapsulation is in up/down state. All incoming packets are errored. This problem occurs when the serial interface is removed and recreated while forwarding traffic.

Workaround: Reload the linecard code using the **hw-module slot <1-8> reset** command.

- CSCef32601

When configuring 1,000 VRFs in a Cisco 10000 series router and injecting 660 static VRF routes per VRF, the route processor cannot hold the total of 660k VRF routes. The CEF is disabled automatically on the router and the router is not able to forward any traffic. When 660 static VRF routes are injected per VRF of 1000 VRFs, the router runs out of memory on the route processor.

If 620 VRF routes per VRF are injected into the router via 1000 eBGP sessions (one eBGP session per VRF), the router runs out of memory on the route processor.

There are no known workarounds.

- CSCef32815

The MQC policer overhead accounting is not consistent between input and output service policies applied to a PPPoA or PPPoEoA virtual-access interface.

There are no known workarounds.

- CSCef36672

The **debug aaa pod** command shows information pertaining to all sessions, not the session you want to end. There is too much information you are not interested in.

There are no known workarounds.
- CSCef42332

The MLPPP peer router reloads after executing the microcode reload pxf command.

This problem occurs when the Cisco 10000 series router crashes when configured with several Multilink interfaces and is passing traffic after a PXF reload on a peer router.

There are no known workarounds.
- CSCef44918

The Cisco 10000 series router shows incorrect counters when executing the **show policy-map interface ATM x vc y** command.

There are no known workarounds.
- CSCef47220

The Path Trace buffer value may be displayed as UNSTABLE, when you do a **show controller** for the AU-3 port and are looking for the overhead bytes.

For a Cisco 10000 series router, the 4-port Channelized OC3 line card is configured as AU-3 E1 configure **j1 length 16** and the AU3 controller is configured **j1 message CISCO SYSTEMS**.

There are no known workarounds.
- CSCef47280

A T1 interface configured under an AU-4 on a 4-port channelized OC3 line card does not come up when interoperating with a 3rd party test analyzer device.

On a Cisco 10000 series router, when you configure the AU-4 T1 interface on a 4-port channelized OC3 line card that is connected to a 3rd party test analyzer device on the far end with the same configuration, the T1 interface does not come up.

There are no known workarounds.
- CSCef47688

When configuring a range of PVCs with more UBR VCs than the limit on the interface, the following error message appears:

```
PVC Range: Total number of VCs exceeds the interface limit.
```

Even if you configure oversubscription under that interface, you cannot configure more circuits than the interface limit.

There are no known workarounds.
- CSCef50661

In some configurations the weight (used for round robin scheduling of the VC into a VP) may be more than the queue depth (the amount of cells the line card will hold for the VC). In this scenario the user may not see the proper weighting of the VCs in the VP. The queue depth places a ceiling on how many cells can be sent at one time.

Workaround: Both the weight and queue depth can be configured with CLI. Ensure that the queue depth is at least as high as the weight.

- CSCef51082
The discard bit match is not done at the MPLS output interface when it is set at the VRF input interface. This problem occurs when the qos set was initially done with the mpls exp bit, then changed to the discard bit.
Workaround: If the discard bit needs to be matched at the MPLS interface, do not configure the mpls exp bit set at the VRF input interface.
- CSCef56348
With PPPoE, PPPoA, or VPDN sessions, the following message may appear in the log: “*Aug 25 06:57:07.759: Reload unknown session type.” This problem can occur after a microcode reload.
There are no known workarounds.
- CSCef56455
On rare occasions, configuring speed using the Dynamic Bandwidth Selection (DBS) feature is not fully reliable. Initial user connections are properly set, but subsequent connections will not. This failure to configure the connection speed using DBS occurs when bringing up over 2,000 user connections.
There are no known workarounds.
- CSCef59264
The IP shaping rate is changed to the VC shaping rate provisioned via DBS. If the VC shaping rate is provisioned via DBS and there is an IP shaper configured in the service policy attached to this VC, the IP shaping rate is set to the VC shaping rate that was provisioned via DBS.
There are no known workarounds.
- CSCef61177
MLPPP traffic is not utilizing full interface bandwidth. This problem occurs when MLPPP and LFI over a serial interface are configured and traffic is sent at the rate of the serial interface or at a greater rate.
There are no known workarounds.
- CSCef61795
F4 OAM cells are not generated or received for end-to-end loopback. Only end-to-end loopback is affected, whereas segment loopback functions as expected.
There are no known workarounds.
- CSCef64315
A traceback can appear when deconfiguring an ATM PVC on a 4-port ATM line card. This problem occurs on a Cisco 10000 series router, on a 4-port ATM OC3 line card.
There are no known workarounds.
- CSCef64378
The Cisco 10000 series router configured and LNS with tos-reflection applied onto the L2TP tunnel towards the LAC drops packets that do not have TOS field=0 on the original IP Header of the packet. Present in Cisco IOS Release 12.3(7)XI with tos-reflect either configured using "ip tos reflect" in the LNS VPDN group.
Workaround: Disable tos-reflection on the VPDN-group on the LNS.

- CSCef69197

When a Cisco 10000 series router is configured for Automatic Protection Switching (APS), a spurious memory access traceback occurs during a router reload. The traceback occurs when one or more pairs of 4 port OC3 ATM line cards are configured for APS, the configuration is saved, and the router is reloaded. There are no subsequent problems related with this traceback.

There are no known workarounds.
- CSCef70580

A Cisco router running Cisco IOS Release 12.3(7)X11 can reload unexpectedly. Output similar to the following is displayed on the console during the reload:

```
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 64A72148 data 64A72AFC
chunkmagic 15A3C78B chunk_freemagic 642A4D04
-Process= "Check heaps", ipl= 0, pid= 5
-Traceback= 608960C8 608962D0 60895F08

%Software-forced reload
Unexpected exception, CPU signal 23, PC = 0x60873608
```

There are no known workarounds.
- CSCef71570

When APS is configured, you see console messages when the PRE2 is rebooted or failed over. There is no impact on the sessions.

There are no known workarounds.
- CSCef72129

When configuring create on demand PVCs (individual and within a range) and PPP sessions, RP CPU utilization can be extremely high when bringing up and tearing down sessions and PVCs. This is only a concern when the configuration contains approximately 30,000 PPP sessions, and additional services are enabled such as DBS, ACLs, and service policies.

Workaround: To reduce the RP CPU usage for PPPoA sessions, reduce the number of configured PVCs in a single subinterface. To reduce the RP CPU usage for PPPoEoA sessions, use call admission control (**call admission limit** command).
- CSCef73055

When switchover is done from the primary PRE2 to the standby PRE2, console messages appear. There is no impact to the system.

There are no known workarounds.
- CSCef74370

At high call rate when the PRE2 is switched over from Primary to Secondary, some of the PTA sessions are stuck in "TRANS" state.

Workaround: Reduce the call rate of the sessions.
- CSCef74990

Broadband PPPoE PTA 28,000 subinterfaces (PVCs) with policy-map, total 114,000 queues, CPU about 62 percent after traffic. This problem occurs when PPPoE PTA 28,000 subinterfaces (PVCs), 114,000 queue scaling configured with traffic.

There are no known workarounds.

- CSCef75434
Inaccurate traffic counters are displayed when running traffic on the Managed LNS router. Cisco 10000 series LNS routers do not match the transmit and receive packets for Managed LNS traffic.
There are no known workarounds.
- CSCef76338
PTA PPPoE 8,000 PVC 32,000 queue, send mixed size line rate traffic, packets drop. Condition: Send mixed size packets line rate traffic, packets tail drop on BQ.
Workaround: Lower the traffic rate.
- CSCef79045
The auto VCs (infinite range VCs) do not disappear even when the traffic from the client is stopped. If traffic is sent on a large number of VCs at a high rate, then infinite range VCs are created, they do not disappear even when the traffic is stopped or the interface is shut down.
Workaround: Stop the traffic and wait for a couple hours for the buffer to clear up and then eventually the VCs to disappear or reload.
- CSCef79688
MPLS Packets are punted to the Route Processor. This problem occurs when MPLS Packets are sent over a Frame Relay Interface.
There are no known workarounds.
- CSCef80300
Enabling multicast on a Cisco 10000 series router working as an LNS causes high CPU usage.
There are no known workarounds.
- CSCef81452
On a Cisco 10000 series router, if the router is configured for Multilink PPP (MLPPP) with QoS and the user resets the line card containing member links, traffic can be affected as a result of the reset. This problem occurs when QoS is configured on MLPPP links and the line card is reset using the **hw-module card x/y/z reset** command.
Workaround: Execute the **microcode reload pxf** command to resolve the problem.
- CSCef81634
Using the external generating tool IXIA Explorer to bring up and tear down SSG sessions quickly, the PRE2 crashes with a Bus Error Exception. This problem occurs when the tool initializes the interface and quickly brings sessions back up while the old sessions are still cleared out.
There are no known workarounds.
- CSCef82322
A line card remains down for more than 10 minutes when you OIR the line card. This problem only occurs with a high number of QinQ sessions (31,000 QinQ sessions).
There are no known workarounds.
- CSCef82371
Changing policy map criteria with a high number of QinQ sessions (31,000) results in CPU-Hog Tracebacks.
There are no known workarounds.

- CSCef83376
When using the VRF to local RADIUS feature that was introduced in Cisco IOS Release 12.3(7)XI1, the default authentication fails, causing the PPPoA or PPPoE session to fail.
There are no known workarounds.
- CSCef84595
The OAM ping sent from the client to UUT, does not get a response back. The UUT was configured with infinite range VCs on the interface. When the client sent an OAM ping packet on one VC to the UUT, the UUT did not create the VC and did not send the response back to the client.
Workaround: If the interface on UUT is configured with no pxf queuing, then the client receives the ping response.
- CSCef84923
The SAR Rev B chip on an OC12 ATM line card reloads multiple times during ATM card reset or boot up. This problem occurs with the latest SAR Rev 1.7.4 running on Cisco IOS Release 12.3(7)XI2 image on a Cisco 10000 series router
There are no known workarounds.
- CSCef85857
E1 interfaces on the 4-Ch-STM1 line card flap randomly. This problem occurs with very little traffic flowing through the router. Whenever the interface goes down, it comes back up after 10 seconds.
There are no known workarounds.
- CSCef89397
On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI, alignment errors occur after executing the **redundancy force-switchover main-cpu** command. This problem was found while running 4,000 active PPPoE sessions and running traffic over some of the sessions.
There are no known workarounds.
- CSCef89413
On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI, there is no message displayed on the router to warn the user that the router has run out of available VCCI interfaces. This problem occurs when more PPPoX sessions come in than there are available VCCIs.
There are no known workarounds.
- CSCef90647
On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI, copying a large file to disk can render the disk unusable. This problem occurs when copying the file on a router with a busy CPU load.
There are no known workarounds.
- CSCef91000
On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI2, when create on demand PPPoE and PPPoA VC classes are configured on the same interface, the PPPoA sessions are not established. This problem occurs only if both PPPoE and PPPoA are configured on the interface with create on demand.
Workaround: Configure different VCs for PPPoE and PPPoA.

- CSCef92161

The absolute priority queue over an MLP bundle drops traffic after policing even when the traffic load is less than the MLP link capacity. This problem occurs when the MLP bundle has more than 1 member and no LFI enabled.

There are no known workarounds.
- CSCef92176

Packets/Bytes counters in the **show interface multilink X** are counted twice. This problem only applies to locally generated traffic, such as ICMP packets.

There are no known workarounds.
- CSCef92261

If large numbers of MPLS VPNs are configured, an SNMP mibwalk of the MPLS-VPN-MIB can timeout and cause a high CPU in the mplsVpnVrfPerfTable and the mplsVpnVrfRouteTable. (This MIB is not supported in Cisco IOS Releases 12.2(16)BX or 12.3(7)XI.)

Workaround: Exclude the mplsVpnMIB (or the mplsVpnVrfPerfTable and mplsVpnVrfRouteTable) from the SNMP view.
- CSCef92404

On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI in RPR+ mode, the microcode of an ATM OC12 line card can reload on PRE failure. This problem occurs only when there is a PRE failure and switchover in RPR+ mode.

There are no known workarounds.
- CSCef92424

The nas-port attribute is not sent correctly while authenticating rfc1,483 users. This problem occurs with a per-server group nas-port configuration enabled on a Cisco 10000 series router, the nas-port attribute [5] is not sent correctly in the access/accounting requests, while bringing up/down rfc1483 users.

There are no known workarounds.
- CSCef92479

Nas-port attribute [5] gets sent out, with 'attribute nas-port none' configured while bringing up ssg rfc1483 users. This problem occurs on a Cisco 10000 series router, where ssg is enabled, and with per-server group nas-port configured. In bringing up rfc1,483 sessions, the nas-port attribute is sent out, despite 'attribute nas-port none' being configured on the router (which should disable sending out of the nas-port attribute).

There are no known workarounds.
- CSCef92614

An incorrect nas-port value is sent out in authentication requests, based on what the configuration on the router was for the same. This problem occurs when the per-server group nas-port has been configured on the Cisco 10000 series router in such a way that the nas-port value in all authentication requests should be sent out in format e string of 32 I's (VPI value of incoming session) and the accounting requests should be sent out in format e string of 32 C's (VCI value of incoming session). However, on session bring up the authentication requests have a nas-port value representing the format e string value corresponding to 32 C's, which is incorrect.

There are no known workarounds.

- CSCef93639

Some Multilink PPP member links turn to up/down after an MR-APS switchover. This problem occurs with T1 interfaces over 4CHOC3 line card on the C10000 platform. The T1 Multilink PPP member links are seen as up/down after a couple of MR-APS switchovers.

Workaround: Resetting the 4CHOC3 line card or reloading the router could bring the interfaces to an up/up state.
- CSCef93866

On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI, the router can reload if high numbers of MLPPP and MR-APS are unconfigured via a tftp configuration file. This problem occurs when a high amount of unconfiguration commands are executed at the same time. This problem occurs with a 4CHOC3 line card while tftp-loading an unconfiguration file to unconfigure a Multilink PPP and MR-APS related running configuration.

There are no known workarounds.
- CSCef94282

On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI, the router could experience longer high CPU Utilization than normal when configuring it with VRFs with VPN overlay. This problem occurs while attempting to bring up 645 PPPoA sessions over 215 VRFs (with VPN overlay) and there are approximately 150,000 BGP routes in the system.

There are no known workarounds.
- CSCef94504

Cisco 10008 router can reload when reporting a software forced crash (memory corruption). The problem was reported in 12.3(7)XI1.

There are no known workarounds.
- CSCef94588

The in/out counters in the output of the **show ip multicast interface** command display only multicast packets punted to the RP for processing. Punted multicast packets are usually control packets. PXF switched packets are not counted in this display.

Workaround: Do **no ip domain server lookup**.
- CSCef94838

On a broadband PTA with 14,336 PPPoE sessions and 43,000 queues, the domain server lookup failure causes a CPUHOG traceback message. This problem occurs when broadband PTA PPPoE queue scaling is configured and domain lookup is enabled.

Workaround: Do **no ip domain server lookup**.
- CSCef95719

RP CPU utilization can be high when bringing up PPPoA sessions when the following features are enabled: 31,500 PPPoA sessions, 12 VRFs, multipoint I/F, pvc (no range), autosense, pxf queueing, vbr-nrt vc shaping, hierarchical shaping, create-on-demand, ACLs (attribute 11), URPF, DBS, and QoS.

There are no known workarounds.
- CSCef95738

RP CPU utilization can be high when sustaining 30,000 PPPoA sessions when the following features are enabled: 12 VRFs, multipoint I/F, pvc (no range), autosense, pxf queueing, vbr-nrt vc shaping, hierarchical shaping, create-on-demand, ACLs (attribute 11), URPF, DBS, QoS, and keepalive 60.

Workaround: The only changeable parameter is the keepalive; turning it off or changing the value to a larger one might improve the situation.

- CSCef96002

No traffic is going out of a few random interfaces on the feed Cisco 10000 series router of an MR-APS setup. This problem occurs with a 4CHOC3 line card on a Cisco 10000 series router that is used as the feed router for an MR-APS setup. Frame Relay is configured on the T1 interfaces and there are two equal weight static routes (one via the MR-APS Working and another via the MR-APS Protect) over each interface for the same traffic destination.

Workaround: Reset the line card or reload the router.

- CSCef96748

The output of the **sh policy-map interface** command shows counter values even before traffic is sent.

There are no known workarounds.

- CSCef96834

Two microcode reloads causes memory corruption and a router reload.

There are no known workarounds.

- CSCef97101

A PXF crash can occur when 3,000 PPPoX sessions are all joining the same multicast group and receiving traffic from a multicast source at a rate of approximately 300 Kbits/sec. The PXF is crashing with the following error in particular:

```
Oct  8 12:51:47.977: %PXF-2-FAULT: T3 XCM1 FCRAM-C: Address Boundary Error
Oct  8 12:51:47.977: %PXF-2-FAULT: T3 HW Exception: CPU[t3r3c1] IWRA at 0x0914 LR
0x090C
Oct  8 12:51:47.977: %PXF-2-FAULT: T3 Local Bus Exception: CPU[t3r3c1] TBNP at 0x0914
LR 0x090C
Oct  8 12:51:47.977: %PXF-2-FAULT: T3 Exception summary: CPU[t3r3c1] Stat=0x00000026
HW=0x00100000 LB=0x00000008 SW=0x00000000
```

There are no known workarounds.

- CSCef97118

On a Cisco 10000 series router running Cisco IOS version 12.3(7)X11, removing an ATM subinterface with an MQC service policy configured and active PPPoA sessions causes the PRE2 to reload. This problem occurs when MAC is configured on the interface.

Workaround: Remove the QoS configuration from the subinterface before removing the subinterface.

- CSCef97194

OC12POS receive interface counters are not accurate. The OC12POS interface counter on the receive side of the MPLS core is reporting almost twice the value than the value reported on the transmit side of the link.

There are no known workarounds.

- CSCef97242

Routers do not use all MPLS loadsharing interfaces to send traffic at the label imposition direction. This problem occurs with MPLS loadsharing and each interface has a unique label.

There are no known workarounds.

- CSCeg00016
 On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI1, the PXF can crash in PTA mode with 8,000 PPPoE sessions configured. This problem occurs when there is a high amount of PPPoE and does not happen in a predictable manner.
 There are no known workarounds.
- CSCeg00190
 When the VT controller is going down/admindown, an incorrect dsx3LineStatusLastChange trap is sent out. This problem occurs when the VT path is configured on the 1choc12-1 or 4chstm1-1 line card.
 There are no known workarounds.
- CSCeg00438
 On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI1, the policer counters in the output of **show policy-map interface** do not increment if the policy map is applied to a Virtual Access Interface. The police conformed/exceeded/violated counters are not updated (values are all zeroes) when an output service policy is applied on a virtual- access interface.
 There are no known workarounds.
- CSCeg01317
 When the resource limitations of cbwfq policy-map are reached, any change to queue limits (even a decrease) displays the “Queue limit failed” error for each and every session on the router.
 There are no known workarounds.
- CSCeg01323
 Even though policy maps are accepted by the console, they do not appear in **sh run** output.
 There are no known workarounds.
- CSCeg01756
 LAC-switched PPPoA sessions do not work when a PVC is configured to use aal5ciscopp as the encapsulation. IPCP negotiation does not complete and PPP keepalives originating at the client timeout. This problem occurs when the Cisco 10000 series router is used as a LAC switch and the PVC is configured to use an encapsulation type of aal5ciscopp.
 Workaround: Use a different encapsulation type on the PVC such as aal5mux.
- CSCeg02916
 With a PRE2 system, when pinging another PRE2 across a serial link with a DSCP service policy attached at both ends and a priority queue designed to match ip dscp default, the outgoing pings go out through the priority queue, but the ping replies come back via the default queue at the remote end (not the priority queue). This is indicated by the **show pxf cpu queue subinterface** command. On the PRE1, the ping replies come back via the priority queue.
 There are no known workarounds.
- CSCeg03962
 PPPoE sessions on standalone VCs don't go down even after the interface is shut down. This problem occurs when PPPoE sessions are created on standalone PVCs, PVC range, and on PVC in range. All sessions are up, and when the interface is shut down all the sessions went down except for the sessions on stand-alone PVCs.
 There are no known workarounds.

- CSCeg03964
 RP CPU utilization can be extremely high when bringing up PPPoA sessions when using I/F Policy Map AV Pairs.
 There are no known workarounds.
- CSCeg04038
 Ping fails across native VLAN1. Dot1Q is enabled between 7500a and esr1 and between esr2 and gsr1. In both the cases the ping fails across the native VLAN1.
 There are no known workarounds.
- CSCeg04052
 Policing CONFORM, EXCEED, VIOLATE counters are incorrect. This problem occurs when attached at an oc48pos interface.
 There are no known workarounds.
- CSCeg05090
 The Cisco 10000 series router reloads upon disconnecting PPPoX sessions. While disconnecting the sessions the CPU utilization is rising to 100 percent (or close) and causing other active sessions to be disconnected. Active sessions being disconnected is also due to the inability of the Route Processor to handle the sending and receiving of the PPP keepalive on these active sessions. The reload is causing an RP switchover but the new active RP is logging the following error messages continuously:

```
Oct 14 17:03:32.401: %C10K-4-LC_WARN: Slot[8/0] loc12atm-1 SAR: 25/190 reassembly
device Get_Channel_Stats failure, status 0x02 (port 0, handle 0x36B3, id 0x0D3E)
Oct 14 17:03:32.925: %C10K-4-LC_WARN: Slot[7/0] loc12atm-1 SAR: 0/54 segmentation
device Get_Channel_Stats failure, status 0x02 (port 0, handle 0x11C7, id 0x00F6)
```

 The reload and unexpected PPPoX disconnection of active sessions is triggered by the termination of some sessions (Terminate-Request packets sent on a few sessions).
 There are no known workarounds.
- CSCeg05765
 The session set up rate for more than 15,000 PPPoA sessions decreases to 1 session/second when all of the VCs are configured on the same multipoint subinterface.
 Workaround: Spread the VCs over several multipoint interfaces subinterfaces.
- CSCeg07002
 The **sh run** command stops working when traffic is sent at 141,000 packets/second on unopened VC's. This problem occurs when trying to test that infinite range VCs are not created when the interface is not configured with 'create on-demand'.
 There are no known workarounds.
- CSCeg09143
 On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI, when member links of an MLPPP bundle flap, some links can fail to join the bundle afterwards and therefore stay in down/down state. This problem occurs only when there are over 1,000 multilink interfaces configured on the router and all flap at the same time.
 There are no known workarounds.

- CSCeg09602
On a Cisco 10000 series router running Cisco IOS Release 12.3(7)X11 and subsequent releases, QoS shaping may not shape to the desired value when used inside a child policy map. This problem occurs only for certain shape values and traffic rates.
There are no known workarounds.
- CSCeg10311
A Cisco 10008 router can crash reporting a software forced crash (memory corruption). The problem occurs in Cisco IOS Release 12.3(7)X11 and seems related to AAA.
There are no known workarounds.
- CSCeg10588
On a Cisco 10000 series router running Cisco IOS Release 12.3(7)X12, the index for oamLoopbackPingCompleted in the oamLoopbackPingCompletion trap is incorrect.
There are no known workarounds.
- CSCeg10833
The CPU stays at 99 percent for quite some time while the CLI command does not return to the prompt. This problem occurs when 16,000 AutoVCs are configured on 16 multipoint interfaces with 1,000 VCs configured in one VC range on every interface. The same VC class is attached to every range. The modification of the queue depth within the VC class causes the CPU hog.
There are no known workarounds.
- CSCeg12977
The Cisco 10000 series router is configured as an L2TP multi-hop router. The AAA authorization does not use the method list and instead uses the default. The tunnel does not get established. This problem occurs only if "aaa authorization default" is configured along with a method list.
Workaround: Configure a method list or configure the default authorization. Configuring both at the same time can cause this problem.
- CSCeg14502
The router ignores the output policy map on a multilink bundle interface for MLPPP-encapsulated packets originating at the router. This problem applies only to locally-originated MLPPP traffic transiting a multilink bundle interface.
There are no known workarounds.
- CSCeg15184
The following errors display when setting up PPPoA sessions under stress:

```
Oct 25 15:37:09.815: %IDMGR-3-INVALID_ID: bad id in id_to_ptr
```


There are no known workarounds.
- CSCeg16612
Invalid authentication requests packet sent out by PRE2 under stress. The invalid packets appear when the CPU is running at 99 percent and approximately 22,000 Active PPPoA sessions.
There are no known workarounds.
- CSCeg16629
The PRE2 is not able to bring up additional PPPoA sessions when the CPU is running under stress.
There are no known workarounds.

- CSCeg16800

Traffic is not received after an MR-APS switchover from the Protect router back to the Working router. Traffic does not resume on the output side of the Working router, after MR-APS switchover from the Protect router to the Working router.

There are no known workarounds.
- CSCeg17057

Changing the queue depth on more than 28,762 VBR PVCs uses all the VCCIs. This problem occurs when traffic is flowing on 30,000 VBR PVCs and the queue depth is changed. This causes the VCCI count to increase and reach the maximum value.

There are no known workarounds.
- CSCeg17829

Ordinary PVCs in a range don't get created after reload. In a PVC range, if the first and last PVCs in range are create on demand and the rest of the PVCs are ordinary PVCs, then on reload the ordinary PVCs don't get created.

There are no known workarounds.
- CSCeg19192

A traceback message displays when you run out of VCCIs while establishing 32,000 PPPoA sessions.

There are no known workarounds.
- CSCeg20293

Packet classification based on the DSCP IP field (or other matching criteria) may not operate as expected in a MPLS VPN configuration with an output service policy applied on an ATM PVC. This problem occurs when packets with a DSCP value set to 'ef' (101110) are transmitted in the downstream direction over a VC onto which an output policy is applied. The DSCP value should trigger the classification in the priority class. Instead, packets get classified in class-default.

Workaround: Toggle the ATM interface by performing a shut/no shut on the interface.
- CSCeg56821

The link should be DOWN between UUT & HP37718 for Frame format pcm31 & crc4.

The test involoves three sub tests.

 - (1) Valid Frame Format Combinations -- CRC4(E1) or SF(T1)
 - (2) Valid Frame Format Combinations -- NO CRC4 (E1) or ESF (T1)
 - (3) Invalid Frame Format Combinations -- pcm31 crc4

The first two sub tests passed. Only third sub test is failed. In the third sub test, invalid frame combinations are configured, and the link should be down once it is configured. But here the link is up.

There are no known workarounds.
- CSCeg71194

PRE2 is not able to bring up additional PPPoA sessions when CPU running under stress.

This issue occurs when the CPU is running under stress.

There are no known workarounds.

- CSCeh06824
C10K: PRE2 PXF may unexpectedly reload with “PXF DMA TBB Length Error”.
There are no known workarounds.
- CSCin74068
When **aaa authen login def enable** and **aaa author exec def gr radius** are configured for a new telnet connection, authentication succeeds (with getting a username) on entering the correct enable password, but an access-request is sent to the RADIUS with NULL username for authorization. Authorization should be suppressed when the username is not known and a RADIUS access-request should not be sent with a null username.
There are no known workarounds.
- CSCin74698
Two accounting stop records are seen when an "rsh" session is established to the router. This problem occurs when **aaa accounting send stop-record authentication failure** command is configured.
Workaround: Disable **aaa accounting send stop-record authentication failure** command if it's not needed.
- CSCsa57481
CLP bit is not set.
This issue occurs in ATM traffic with CLP bit set.
There are no known workarounds.
- CSCsa62204
Label switching might fail for VPN routes.
This issue has been observed on Cisco 10000 series routers running Cisco IOS Release 12.2.16BX and having E3 card.
There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(7)XI3

This section describes caveats that were fixed in Cisco IOS Release 12.3(7)XI3.

For information about caveats fixed in other Cisco IOS releases, refer to the appropriate Release Note document at the following URL:

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

- CSCed65778

Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the Cisco IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on Cisco IOS devices, may contain two vulnerabilities that can potentially cause Cisco IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml>

- CSCed78149

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCee67450

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. Only devices with the command `bgp log-neighbor-changes` configured are vulnerable. 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.

Cisco has made free software available to address this problem.

This issue is tracked by CERT/CC VU#689326.

This advisory will be posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

- CSCef44225

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef60659

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef61610

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef67682

Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at <http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml> contain fixes for this issue.

- CSCef68324

Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

Cisco has made free software available to address this vulnerability for all affected customers.

More details can be found in the security advisory that is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

- CSCeg31378

Errors and tracebacks occur when ATM pvc creation is initiated but details are not entered.

The errors and traceback only occur when the Cisco C10000 series router is forced to default the pvc configuration details.

Workaround: Enter PVC definition information immediately when entering PVC creation.

- CSCeg32441

A performance degradation may be perceived when Hierarchical VP/VC shaping is configured. In case a VP is overloaded, output drops may occur at the SAR level and affect all configured shaped VPs on the interface.

This issue is seen with a configuration that includes 4 shaped VPs and 800 active VCs within each VP.

There are no known workarounds.

- CSCeg34984

When an existing create on-demand vc is added with PPPoA encapsulation, it automatically comes up, provided there are some existing PPPoA sessions in the same main interface.

There are no known workarounds.

- CSCeg37235

Although the maximum number of VCs per OC3 and DS3 ATM line card has been extended to 28,672 in Cisco IOS Release 12.3(7)X12, the maximum number of VCs within VPs that can be supported on the ATM DS3 and OC3 line cards is only 22,204. ATM errors occur when attempting to bring up more than 22,204 VCs in a configuration that includes shaped VPs and VCs (Hierarchical Traffic Shaping).

This problem is seen with a configuration that includes shaped VPs and VCs (Hierarchical Traffic Shaping).

Workaround: Limit the number of configured VCs on the ATM module to less than 22,204.

- CSCeg37696

A Cisco 7200 series may unexpectedly reload when a script configures MVPN.

This issue is observed on a Cisco 7200 series running Cisco IOS Release 12.3(6d) and that is configured with an NPE-G1.

There are no known workarounds.

- CSCeg37903

When using PPPoA where late adjacencies may occur. Such events often correspond to the selection of TAGs associated with RA-MPLS and/or HDX- VRF configurations. When such an event occurs, the PPPoA connection will exhibit a spontaneous clearing of the connection counters.

The **show int virtual-access x.x** and associated commands will not reflect an accurate accounting of packet traffic through the PPPoA session.

There are no known workarounds.

- CSCeg38185

When no username and no password are provided during PPP authentication (PAP), the authentication will fail with message password too long in the PPP state machine.

Workarounds: Use a single char username, a single char password, or remove ppp authentication.

- CSCeg38220

All VRF packets forwarded using default route entry will go out with only IGP label and do not have the VPN label. Hence, remote PE will not be able to forward them to remote CE.

This issue occurs when there is IGP loadbalancing to reach remote PE, and static default route is configured on a local Cisco 10000 series PE router with next hop as remote CE's loopback address. This causes double recursion since remote CE's loopback address can be reached via remote PE's loopback address.

Workaround: Disable IGP loadbalancing between local PE and remote PE.

Alternative Workaround: Have the remote CE (or the remote PE attached to that CE) advertise the default route via BGP to the local PE.

- CSCeg38795

The number of flowbits allocated to a PVC is not updated upon changing the PVC rate via the Dynamic Bandwidth Selection (DBS) feature.

This issue occurs when the Peak Cell Rate (PCR) and Sustainable Cell Rate (SCR) of the vbr-nrt pvc are dynamically changed via DBS.

Workaround: Disable DBS.

- CSCeg38937

After a PRE force-switchover, counters on the ATM interfaces do not get incremented. Though the VCs are up and traffic is flowing, the counters happens to be null and not incrementing.

This issue occurs in Cisco IOS Release 12.3(7)XI running on a Cisco 10000 series router.

Workaround: Once reset, the ATM linecard counters on the ATM interfaces seem to be operational.

- CSCeg39011

The **show redundancy states** command shows Redundancy Mode (Configured) = Hot Standby Redundancy.

The mode should be Route Processor Redundancy Plus.

When using redundant PRE-2, the **show redundancy states** command shows the incorrect Redundancy Mode (Configured).

There are no known workarounds.

- CSCeg40706

The router unexpectedly reloads when migrating PPPoA clients from one VAI (Virtual Access Interface) to another.

This issue occurs when changing the type of the vaccess interface from sub-VAI (ex. vi1.4) to a full VAI (ex. vi5).

There are no known workarounds.
- CSCeg41293

The RP may unexpectedly reload because of some event scheduler data being corrupted. The following message appears on the console:

```
*Nov 23 15:59:15.340: %SCHED-3-CORRUPT: Scheduler 'event magic' corrupted by
process Check heaps (expected DEADFEED, found 0)
-Process= "Check heaps", ipl= 0, pid= 5
-Traceback= <truncated>
```

This issue is a very rare event. The trigger is unknown.

There are no known workarounds.
- CSCeg41800

PPPoX sessions and ATM VCs are torn down upon modifying the over-subscription-factor. Furthermore, the VCs will remain in INAC state upon attempting to re-establish the sessions.

This issue occurs in a configuration that includes shaped VPs and VCs (Hierarchical Traffic Shaping) after increasing the atm over-subscription-factor.

There are no known workarounds.
- CSCeg41929

A 10008 may report some packet drops upon reload.

The issue is observed in Cisco IOS Release 12.3(7)X12 when a policy map is applied on a virtual template. The trigger is the reload of the router.

Workaround:

 1. Downgrade to Cisco IOS Release 12.3(7)X11.
 2. Apply the policy map via radius.
 3. Reapply the service policy on the virtual template after reload completes.
- CSCeg42877

PPPoA sessions are not coming up in autovcs after shut/no shut and tracebacks are reported

This issue is found only if the QoS parameters are configured via Radius server

Workaround: The QoS parameters can be configured through CLI.
- CSCeg44467

When the router is setting up a large quantity of PPPoX sessions simultaneously, the router may unexpectedly reload when it tries to install a per user idle timeout.

This condition only occurs with large scale aggregations of PPPoX sessions and with the idle-timeout radius-attribute being configured through radius.

Workaround: Do not send the Att28 from radius to the router when the router is simultaneously bringing up large quantities of PPPoX sessions.
- CSCeg45350

High CPU utilization when PPP sessions are up.

This issue occurs in PPPoX sessions with many features turn on (such as DBS, HDVRF, URPF, QoS).

There are no known workarounds.

- CSCeg45430

The class attribute is not included in the accounting request when vpdn-authen-before-forward is configured.

The issue is the class attribute missing in the ACCOUNTING request. Not doing preauthentication or downloading. The issue is that the user authentication results in an access-reply with the class which is sometimes not included in the accounting request.

Workaround: Issue the **aaa accounting delay-start** command.

- CSCeg45795

The router may unexpectedly reload when ATM idle timeout expires.

This issue is observed with auto VC and QoS are configured.

Workaround: Either use large idle timeout or do not use autoVC.

- CSCeg47701

The router may unexpectedly reload with a bad block pointer error when running Cisco IOS Release 12.3(7)XI2.

There are no known workarounds.

- CSCeg48126

The following messages appears on the console:

```
%C10K-2-BADRSRCNUM: Invalid resource number from PXF (15). (PLEASE REPORT THIS!)
```

This occurs with APS configured Fail over is executed from Active to Standby

There are no known workarounds.

- CSCeg48245

The scr value for vbr-nrt VCs can be set to a value below 38 when configuring through vc-class.

This issue occurs with unexpected tracebacks and dynamic service-policy problems

Workaround: change the vc-class from “vbr-nrt 38 0” to “vbr-nrt 38 38 50”.

- CSCeg48971

The command to display cached PPPoE configuration information is present in Cisco IOS Release 12.3T but not in Cisco IOS Release 12.3(7)XI3.

The affected command is **show pppoe derived**. The command is not present in Cisco IOS Release 12.3(7)XI3.

There are no known workarounds.

- CSCeg50631

C10k-3-LC_ERROR messages flood the console.

This issue occurs when oc-3-atm line cards are removed/associated from redundancy.

There are no known workarounds.

- CSCeg53972

A router terminating PPPoA sessions which have QoS applied may print the following messages when clearing the sessions:

```
Dec 13 13:27:50.608: Assertion failure in
../toaster/c10k_rp/c10kds2_qos.c:write_primary_police_data_index() (4247)
Expression 'first_if_info->qos.police_data[policy_index].size' = 0x0
```

There are no known workarounds.

- CSCeg53998

PRE2 may generate the following errors when setting up PPPoA sessions when CPU running under stress:

```
Dec 13 12:47:54.976: %C10K_QOS_GENERAL-3-EREVENT: Error @
../toaster/c10k_rp/c10kds2_qos.c:c10k_pppox_un_inherit_qos() line:
```

There are no known workarounds.

- CSCeg55523

A memory leak may occur in the ATM Auto-VC creation process.

This issue is observed on a Cisco 10000 series that is configured for dynamic bandwidth selection (DBS) but may also occur on other platforms.

There are no known workarounds.

- CSCeg56225

With Cisco IOS Release 12.3(7)XI2, the message “%ATM-3-FAILCREATEVC: ATM failed to create VC - (Cause of the failure: VC Creation has failed due to a platform-specific limit)” and “Attempting to over- subscribe tunnel bandwidth” messages may erroneously be logged

This issue occurs when changing parameters at the PVC level.

There are no known workarounds.

- CSCeg57904

The router may unexpectedly reload due to memory corruption.

There are no known workarounds.

- CSCeg58833

The router unexpectedly reloads when removing a v-template from a router with active multi-cast interfaces running.

This issue occurs on any Cisco IOS release running multicast on v-template interfaces.

Workaround: Either remove the multicast configuration from the v-template prior to v-template removal, or disable interfaces prior to removing the configuration.

- CSCeg60483

Multicast ping failed with sparse mode in Multicast VPN case.

The Multicast VPN failure is observed in sparse mode only

There are no known workarounds.

- CSCeg60659

ATM oversubscription factor of 50 is maximum.

This issue occurs on C10K PRE2 with any software.

Workaround: Use UBR VCs when using Cisco IOS Release 12.3(7)XI2 or later and UBR VCs service policies can also be attached, and there is no need for an over subscription factor. SCRs from VBR are deducted from the interface BW. This is not the case with UBR.

- CSCeg61244

Template down loading may not work with CSCee52915 featurette.

If VPDN tunnel is established with template down-loading feature with method-list and AAA specific configuration, then incoming user request is forwarded to the default mlist instead of template specific.

There are no known workarounds.

- CSCeg61586

A router may reload when PPPoA sessions are being established or torn down.

This issue is observed when the configuration of the ATM interface over which the sessions are received is altered.

There are no known workarounds.

- CSCeg61668

If a change is made to the ATM clocking on the main interface either immediately after or immediately before configuring a “create on-demand” VC on a P2P sub-interface (within or outside of a vc-class), the VC is created and comes up right away.

Workaround: If configuring ATM clocking on a main interface on which create-on-demand VCs will be configured, then wait a few seconds after configuring clocking, before configuring the VCs. If configuring the VCs first, then wait a few seconds afterwards, before configuring atm clocking.

- CSCeg63963

Incorrect reporting of OC3/OC12 bandwidth in the output of the **sh atm int atm x/y/z** command and the log message when one exceeds the interface bandwidth.

This issue occurs on an ESR 10008 when oversubscribing an ATM interface one may see incorrect reporting of OC3/OC12 bandwidth in the output of the **sh atm int atm x/y/z** command and the log message when one exceeds the interface bandwidth.

There are no known workarounds.

- CSCeg65883

C10K: PRE2 may unexpectedly reload when collecting statistics.

This issue is observed in the script used for applying the service policy under the Virtual-Template.

The PRE2 may unexpectedly reload with the following context:

```
10000 Software (C10K2-P11-M), Experimental Version 12.3(20041202:192054)
[xthuijs-V123_7_XI2_TI 100]
Compiled Thu 02-Dec-04 14:52 by xthuijs
Signal = 10, Code = 0x10, Uptime 23:13:47
$0 : 00000000, AT : 62300000, v0 : 62CF6244, v1 : 00000000
a0 : 62CF6244, a1 : 0E194A5F, a2 : 00000001, a3 : 6245E508
t0 : 229EDFFC, t1 : 229EDFBC, t2 : 6245E50C, t3 : 60483EF0
t4 : 60483EF0, t5 : 00000000, t6 : 00000020, t7 : 0000FF00
s0 : FFFFFFFF, s1 : 04FBE
8F4, s2 : 00000000, s3 : 00000004
s4 : 72F21B0C, s5 : 00000000, s6 : 63E940C8, s7 : 229EDF5C
t8 : 229E688C, t9 : 00000000, k0 : 635AD638, k1 : 6046D288
gp : 62303408, sp : 70A1CA88, s8 : 72F21AD8, ra : 60D53C64
EPC : 60D53C94, SREG : 3400FF03, Cause : 00000010
Error EPC : C7683125, BadVaddr : FFFFFFFF
```

```
CacheErr : 00000000, DErrAddr0 : 00000000, DErrAddr1 : 00000000
ECC : 00000000, INFO : 34082084
```

There are no known workarounds.

- CSCeg66395

VC parameters were not set with the correct received values.

This issue may occur when DBS is receiving parameters from the Radius server.

Workaround: Touching the vc config resolves the issue.
- CSCeg66691

Once the interface is oversubscribed on an ATM interface that is down, the overwriting of the VP with a peak rate that is less than the available bandwidth is ignored.

Workaround: Make the change when interface is up.
- CSCeg68050

VP PCR rates are not checked against the oversubscribed bandwidth of an interface.

This issue occurs on an oversubscribed ATM interface with VP PCR rate setting.

There are no known workarounds.
- CSCeg68959

Packet 5 expected to be diverted for clns_isis was not found.

When tested with various Cisco IOS Release 12.3(7)XI images and up to 2004-11-21 dated image, the test was passed. After that, only the test starts failing.

There are no known workarounds.
- CSCeg70485

After executing failover from active to standby PRE2, the standby PRE2 may unexpectedly reload while booting.

The exact cause is still needs to be identified. This is reported/seen under the below conditions:

 - 40K PVCs create-on-demand are spread across 12 oc3 interfaces. APS is defined for all 12 oc3 interfaces.
 - VP/VC (vbr-nrt) shaping is used on all of them.
 - 18,000 PTA sessions are up.

There are no known workarounds.
- CSCeg72050

No VCs are created after OIR.

This issue occurs with hw-module shut/unshut.

There are no known workarounds.
- CSCeg73482

ATM interface does not come up while running 8e3ds3atm tests.

This issue is observed while running 8e3ds3atm linecard regression scripts.

There are no known workarounds.
- CSCeg73739

In Multilink PPP (MLPPP), the first packet is received in the wrong order.

This issue occurs only for the first MLPPP packet. Other packets are sent in the right order.

There are no known workarounds.

- CSCeg73871

The startup-config file open failed when the **show startup** command is executed. This appears each time when a vty session on which **show startup** or **show conf** is executed but not finished. The config could not be saved.

There are no known workarounds.

- CSCeg73960

The router may unexpectedly reloads on the **clear counters** command with policy map applied to subinterface VCs.

This issue occurs on dynamic policy maps.

There are no known workarounds.

- CSCeg74331

Upon rare occasions, PPPoX users using DBS (dynamic bandwidth selection) will not get the DBS allocated bandwidth applied. This only occurs when the PVC configuration is done ten seconds or less before the PPPoX user authenticates.

There is a race condition where, if an ATM PVC is added to the configuration and a PPPoX user immediately attempts to authenticate, DBS is not applied to the resulting PPPoX user PVC.

Workaround: Configure PVCs prior to applying users to them. If an ATM PVC configuration must be deleted and added back, then prevent users from attempting to authenticate for ten to fifteen seconds to allow the PVC configuration to complete in the router.

- CSCeg74196

All interfaces do not go down when far end is shut down in the 8e3ds3 linecard tests.

This problem does not occur in Cisco IOS Release 12.3(7)X13.

There are no known workarounds.

- CSCeg74992

On Cisco 10000 routers running Cisco IOS Release 12.3(7)X12 and later, the values for percent-based policing once applied to an ATM VC are not calculated properly and therefore do not reflect the configured values.

There are no known workarounds.

- CSCeg75281

A PPPoE test client with Cisco IOS Release 12.3(7)X13 may unexpectedly reload if generated circuit-id tag is 99 bytes long.

Workaround: Test the feature by generating tags which are not 99 bytes long. The maximum allowed tag length as per DSL forum is 48 bytes, so this defect should not cause any hindrance in feature testing.

- CSCeg77405

Sometimes SAR Page Limitation of 510 pages cannot be achieved except if the router is reloaded. The following error from the line card is displayed and then only 256 VCs come up:

```
config VC reassembler, channel descriptor allocation failure
```

Workaround: Reload the router.

- CSCeg78564

VPs bandwidth reserving and releasing is not handled correctly for the following cases:

- shut/no shut of the ATM interface
- soft/hard reset of the ATM card

This issue occurs in Cisco IOS Release 12.3(7)XI running on a Cisco 10000 series router.

There are no known workarounds.

- CSCeg79684

The various show commands of Radius statistics are missing the number Access-Rejects.

This issue occurs when radius is in use and Access-Rejects are received.

Workaround: Count the number of Access-Rejects yourself with debug radius.

- CSCeg79865

The customer requirement is to limit the number of PPPoE sessions available for each QinQ inner VLAN. This is somewhat supported using the sessions per-vlan limit command option under the PPPoE bba-group. However the way this works is that individual QinQ subinterfaces have to be created for each QinQ inner vlan tag. This is clearly stated on CCO that it works this way.

This means that a very large configuration has to be done if a number of QinQ inner vlan tags are used. Basically one sub-interface need to be created for each QinQ inner vlan tag used. If 32,000 QinQ inner vlan tags are used then 32,000 sub-interfaces will need to be created. This is not acceptable by the customer and most customers would not accept this.

A more acceptable configuration would be to use the ANY option for the QinQ inner vlan tag and have the session per-vlan limit work, such as the following:

```
bba-group pppoe group1
sessions per-vlan limit 1
!
interface GigabitEthernet8/0/0.1
 encapsulation dot1q 2 second-dot1q any
 pppoe enable group group1
```

Unfortunately using ANY as the inner vlan tag option does not work as is required. In this case it will only limit PPPoE sessions on the first QinQ inner vlan tag that is detected. Any PPPoE sessions that try to come up on any other QinQ inner tags will be rejected. This is not what was expected.

It is expected that at one PPPoEoQinQ session will be allowed on each QinQ inner vlan tag.

There are no known workarounds.

- CSCeg84029

This DDTS is to try to introduce the functionality to reflect the IP TOS values automatically into the Ethernet COS field without the need to build egress policy-maps on each Ethernet interface, specifically setting the values.

Workaround: Use policy-maps to copy the IP TOS to L2 COS.

- CSCeg84454

When changing a policy map for policy “COLA64” with 60,00 PPPoE sessions active as a PTA, no traffic No Service policy is applied.

When 10,000 PPPoA sessions are active as a LACm, no traffic and policy “COLA64” is applied to all.

When 7,500 RFC1483 are active as PTA, no traffic and policy “COLA64” is applied to all.

When the policy map is changed from the following:

```
c10c8-1#sh policy-map
  Policy Map COLA64
    Class class-default
      queue-limit 64
```

To add a new class with Priority, ACTIVE PRE is lost due unexpected reloads of the software:

```
c10c8-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
c10c8-1(config)#policy-map COLA64
c10c8-1(config-pmap)#Class realtime
c10c8-1(config-pmap-c)# priority
```

Workaround: Remove the policy map from the VCs, and reapply the policy map. Avoid modify the policy map when it is attached to the VCs in a large scale config.

- CSCeg85061

Unable to use **protocol pppoe group** *group_name* command inside a vc-class to point to the bba-group for PPPoE sessions.

The **protocol pppoe group** *group_name* command is not available under the vc-class configuration mode.

Workaround: Directly apply the command under the interface configuration mode.

- CSCeg85823

On an interface, if there is a range of PVCs with regular (ordinary) VCs, and in that range there is a pvc-in range but this pvc-in range is auto vc, then the ordinary VCs do not come up

This issue is only seen when there is a combination of ordinary and autovcs in a range.

There are no known workarounds.

- CSCeg86096

Policy map does not get deleted from Virtual Template.

This issue occurs when policy map is applied to VT.

There are no known workarounds.

- CSCeg88940

When configured for APS, if the active card is removed, it is not possible to transmit traffic to a far end; but transmitting from the far end is ok.

This issue is observed on a Cisco 10000 series OC3ATM card.

There are no known workarounds.

- CSCeg89144

The aaa syslog error for a buffer overflow message does not report the attribute that caused the problem.

The message is seen when a certain attribute exceeds the buffer allocated for a radius packet that Cisco IOS generates.

There are no known workarounds.

- CSCeg89818

When remote end is down, the router is sending LRDI on active APS channel.

This issue occurs when shutting down the remote end.

There are no known workarounds.

- CSCeg90756

Unable to configure a PVC range on a p2p ATM interface, even after previous PVC range configuration is removed.

This issue occurs when the following is performed:

1. Apply a PVC range on ATM p2p interface
2. Unconfigure the previous configured one
3. Apply a new PVC range

This issue is not seen on a multipoint interface.

There are no known workarounds.

- CSCeh00755

Add support for QoS to LAC based sessions. The QoS is applied to the VC where the session come in on.

There are no known workarounds.

- CSCeh00886

When the **show controller t3 ###/## detail t3framer** command is issued, the following tracebacks are displayed, all serial interfaces go down, then the router reloads:

```
L1.3.6-10008-A#sh controllers t3 5/0/3.1 detail t3framer
```

```
%ALIGN-1-FATAL: Corrupted program counter
pc=0x0, ra=0x0, sp=0x204EFD20
```

```
%ALIGN-1-FATAL: Corrupted program counter
pc=0x0, ra=0x0, sp=0x204EFD20
```

```
Unexpected exception, CPU signal 10, PC = 0x0
```

```
-Traceback=
```

```
$0 : 00000000, AT : 62300000, v0 : 00000000, v1 : 00000001
a0 : 00000000, a1 : 00000000, a2 : 622FB7C0, a3 : 00000001
t0 : 60486798, t1 : 3400FF01, t2 : FFFF00FF, t3 : 60486790
t4 : 60486790, t5 : 00020B22, t6 : 00000008, t7 : 0000FF00
s0 : 00000000, s1 : 00000000, s2 : 00000000, s3 : 00000000
s4 : 00000000, s5 : 00000001, s6 : 00000001, s7 : 00000000
t8 : 0D0D0D0D, t9 : 00000000, k0 : 3040F001, k1 : 08200014
gp : 62303408, sp : 204EFD20, s8 : 00000000, ra : 00000000
EPC : 00000000, ErrorEPC : F1EAD5E3, SREG : 3400FF03
MDLO : 00000000, MDHI : 00000000, BadVaddr : 00000000
CacheErr : 00000000, DErrAddr0 : 00000000, DErrAddr1 : 00000000
Cause 00000008 (Code 0x2): TLB (load or instruction fetch) exception
```

```
Unexpected exception, CPU signal 10, PC = 0x0
```

```
-Traceback=
```

```
$0 : 00000000, AT : 62300000, v0 : 00000000, v1 : 00000001
a0 : 00000000, a1 : 00000000, a2 : 622FB7C0, a3 : 00000001
t0 : 60486798, t1 : 3400FF01, t2 : FFFF00FF, t3 : 60486790
t4 : 60486790, t5 : 00020B22, t6 : 00000008, t7 : 0000FF00
s0 : 00000000, s1 : 00000000, s2 : 00000000, s3 : 00000000
```



```
s4 : 00000000, s5 : 00000001, s6 : 00000001, s7 : 00000000
t8 : 0D0D0D0D, t9 : 00000000, k0 : 3040F001, k1 : 08200014
gp : 62303408, sp : 204EFD20, s8 : 00000000, ra : 00000000
EPC : 00000000, ErrorEPC : F1EAD5E3, SREG      : 3400FF03
MDLO : 00000000, MDHI      : 00000000, BadVaddr : 00000000
CacheErr : 00000000, DErrAddr0 : 00000000, DErrAddr1 : 00000000
Cause 00000008 (Code 0x2): TLB (load or instruction fetch) exception
```

This problem occurs on a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI2.

Workaround: Do not issue the command **show controller t3 ###/### detail t3framer** command.

- CSCeh03823

CLI based service policy update on VC should be done through modify path, not through re-create path. As the service policy update on VC does not need VC to be teardown and created in the line card. Also, the router has the dynamic modify path implemented for VC. The ATM common code changes would be done under CSCeh00755, and the platform changes would be done under this DDTs.

This issue occurs when QoS is in use and changed under the VC.

There are no known workarounds.

- CSCeh04524

Configuring or modifying ISIS parameters are not synchronized to the secondary PRE, leaving the running configuration out of sync with the redundant PRE.

This issue occurs on redundant systems running Cisco IOS Release 12.3(7)XI2b.

Workaround: After the ISIS parameters are modified the secondary PRE can be reset (via the **hw-module sec-cpu reset** command) which will allow the secondary to be updated with the latest configuration since this problem does not occur when the secondary receives its configuration during initialization.

- CSCeh07013

The router may experience a high CPU load of 99 percent while setting up sessions. This may be experienced in ANY configuration, LAC/PTA/LNS with or without qos and regardless of the PXF queuing mode or (ATM) interfaces where the sessions come in on.

This issue occurs if there are too many VCs configured under a multipoint interface.

Workaround: Cisco recommends configuring no more than 1500 VCs per multipoint interface. This gives the best scaling results for the Cisco 10000 series router.

- CSCeh07440

The **<no> router isis** command and subsequent commands in “(config-router)” mode may not be correctly synchronized to the standby/secondary PRE when the standby is up and receiving line-by-line running config sync. This may result in the standby being incorrectly configured. This only happens when the standby is up and the ISIS configuration is being modified on the active.

Workaround: If the ISIS configuration must be changed on the system, the standby PRE should be reset after the reconfiguration of “router isis” is completed. By resetting the standby (via the **hw-module sec-pre reset** command) the standby will reload and receive the new ISIS configuration via bulk sync when reinitializing. The bulk sync mechanism does not have this problem.

- CSCeh08171

Interface counters on Gigabit Ethernet interfaces do not increment properly when the interface is configured for VLANs and QinQ.

This issue occurs when the interface is configured for VLANs and QinQ traffic.

Workaround: Statistics are accurately being reported into SNMP MIB counters, which are available through network management applications.

- CSCeh08271

Traffic is lost or traffic is not shaped properly or traffic throughput performance not as expected.

These issues will occur when the pcr/scr of a non-aggregated PVC is changed on the fly.

Workaround: Delete the affected PVC and recreate it.

- CSCeh08472

The LAC-QoS test scaled to 31,000 subscribers with QoS policy configured on ATM VCs and seemed to remain up OK. The ATM VCs have DBS enabled and idle-timeout of 60 second configured. While start bringing down the sessions, the router may unexpectedly reload.

This issue occurs in Cisco IOS Release 12.3(7)XI running on a Cisco 10000 series router.

There are no known workarounds.

- CSCeh09443

The PXF dontfrag counter does not properly increment when the do not fragment bit is set in the packet. The affected counter can be viewed with **show pxf cpu stat ip | incl dontfrag**.

The dontfrag counter only increments when the do not fragment bit is set.

There are no known workarounds.

- CSCeh14800

The ESR10000 PRE2 can experience L2TP session drops while sending traffic through the sessions.

There are traffic shaping and QOS. The 160,000 PTA and L2TP sessions are distributed to 4 OC3 interfaces (2 line cards). The LNS is also an ESR10000 PRE2. One of the OC3 has both PPPOE-PTA and PPPOA-L2TP.

There are no known workarounds.

- CSCeh14826

OC3 line card becomes unresponsive and down. It is stuck in initialization state.

This issue is trigger when HA cut over 3-4 times.

Workaround: Use the **hw-module reset** command.

- CSCin78805

When Auto VCs are configured as part of a range on a point-to-point subinterface, the VCs are made inactive.

There are no known workarounds.

- CSCin82407

Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

- CSCin84978

High CPU utilization is observed. when large number of VCs are configured on the multipoint.

This issue occurs when large number of PVCs are configured on the multipoint subinterface and PPPoA sessions associated with the VCs download the service policy from the Radius server, high CPU utilization is observed.

Workaround: Configure less number of PVCs on the multipoint subinterface.

- CSCin85191

Add support for QoS to LAC based sessions. The QoS is applied to the VC where the session come in on. This was previously not supported/operational.

There are no known workarounds.

- CSCin86689

Auto VCs on the DOWN interface remain INACTIVE.

If a range of PVCs is configured on an interface which is DOWN and then converted to range of AutoVCs, the Auto VCs remain INACTIVE.

Workaround: Shut/no shut the main interface. This will force the PVCs to be properly torn down and recreated in the new configuration.

- CSCin86967

Configurations which are begun, but not completed, at the time of a Cisco 10000 PRE2 Primary switchover can become locked and cannot be edited or deleted.

SVC configurations have been known to become locked if the Cisco 10000 primary PRE2 fails over to the secondary PRE2 prior to exiting the PVC/SVC bundle configuration mode.

Workaround: Since the SVCs and bundles were in the process of being created at the time of Primary PRE2 failover, no users are directly affected.

Reroute the affected configuration to new SVC bundles in order to complete the configuration. Delete the locked and incomplete configuration after the next Primary PRE2 failover.

- CSCin87825

Initial configuration of auto-provisioned PVCs with idle-timeout can, upon occasion, result in PPPoE sessions not coming up.

This issue is observed when PVCs are configured with auto-provisioning enabled (create on-demand), along with idle-timeout, the PPPoE sessions will not initially bring up the PVC.

Workaround: When a PPPoE session does not properly make a PVC active, unconfigure auto-provisioning and unconfigure idle-timeout. Wait for the session to become active, and configure auto-provisioning and configure idle-time on the PVC.

- CSCsa42534

Syslog messages are not issued when individual radius servers become unresponsive.

This issue is observed when a group of radius servers are used to service a router, if an individual radius server does not respond, a console log message will occur, but no syslog message will be issued.

If all Radius servers are found to be unresponsive, a console log message will occur, and a syslog message will be issued.

Workaround: For syslog driven management systems, there are no known workarounds.

- CSCsa43885

Create on-demand PVCs will not be torn down if the interface is shutdown. If the PVCs idle-timeout while the interface is up, then the PVCs will be torn down. The PVCs will be visible as INAC PVCs in **show atm vc** commands.

PVC structure information is retained when an interface is shutdown. When PVCs are created on-demand and the interface is shutdown, Cisco IOS does not know whether the PVC should be torn down until the interface is returned to an up state.

There are no known workarounds.

- CSCsa44473

GigE interface stays down during flow control negotiation.

This issue is observed on a GigE on Cisco IOS Release 12.3(7)XI.

Workaround: Disable flow control (no nego auto under the gige interface).

- CSCsa46561

The router unexpectedly reloads with a rapid disconnection of sessions.

The router unexpectedly reloads with the following traceback after going out of the Adtech configuration and back in again, which triggers the Adtech cards to re-initialize, with sessions connected (3 STM-4 ATM interfaces with each 7800 session):

```
FP: 0x64FF3850, RA: 0x6019CF88
FP: 0x64FF3880, RA: 0x6019DA98
FP: 0x64FF38A8, RA: 0x6019EE80
FP: 0x64FF3B48, RA: 0x60162A58
FP: 0x64FF3DE8, RA: 0x60C75C6C
FP: 0x64FF3E20, RA: 0x60C75E34
FP: 0x64FF3E38, RA: 0x60C72F18
FP: 0x64FF3E58, RA: 0x60C6A248
```

There are no known workarounds.

- CSCsa46626

PPP PADT messages are not sent by a PPPoX PTA router to a client when the PPPoX user is no longer connected to the PPPoX PTA router.

This feature is enabled only within the BBA Group configuration using:

```
bba-group pppoe pppoe1
sessions auto cleanup
```

This issue can occur when a Cisco 10000 Series router is used as a PPPoX PTA router, and there has been a network flap causing the PPPoX users to lose their connections. PPPoE will experience this issue when BBA Groups are in use. VPDN Group configuration does not support this feature.

There are no known workarounds.

- CSCsa46838

When a session established or disconnects with DBS, the following error message is generated:

```
Dec 6 16:32:21: %C10KATM-3-DBS: C10K internal DBS error, DBS: modify()
failure: validation of params unsuccessful(1) ATM3/0/0 8 1/55
-Traceback= 60087ACC 60086D74 60162AA0 60C7566C 60C75804 60C74CD4 60C754A4 6086F7B0
6047DAA4
6047DC00 6045FF5C
```

This issue only occurs in low VC mode.

There are no known workarounds.

- CSCsa49794

The following behaviour is seen, when during a “aaa route download” the Radius server becomes unavailable and available again and the route download is started again that the router starts sending aaa accounting messages to the tacacs-server.

After the that it keeps logging to the TACACS+ server. The only way to recover is to remove the accounting commands or reload the router.

This situation happens when the following commands are configured:

```
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
```

Workaround: Remove the accounting commands or reload the router.

- CSCsa50440

PXF may reload unexpectedly with the following error:

```
PXF DMA Error - End of Descriptor Before Cmd Byte Length Exhausted
```

This unexpected reload is observed on a Cisco 10008 router running Cisco IOS Release 12.2(16)BX3. The unexpected reload occurs when a packet with DF bit set enters an interface with an access-list configured, and leaves the router with an L2TP encapsulation AND the L2TP encapsulated packet is larger than the egress interface MTU.

Workaround: Removing the access-list on the ingress interface stops the PXF reloads.

- CSCsa50532

The counters you get with the **show aaa server-private** command are incorrect. Requests and transactions are counted twice.

This issue occurs when AAA and Radius are configured and utilized.

There are no known workarounds.

- CSCsa50572

NAS port attribute is incorrect and the nas-port is missing in session-id attribute in RADIUS access-request and accounting requests for connections to a proxy SSG service.

When a PPPoEoE SSG user logs in to a SSG proxy service, the NAS-port attribute is sent as “0” and is also not added to the session-id in the access-request and accounting records for the connection.

There are no known workarounds.

- CSCsa51148

When using the **t1 yellow** commands under the controller, the first attempt is ignored.

This issue occurs when configuring the **t1 yellow** commands under the controller.

Workaround: Enter the **t1 yellow** command twice.

- CSCsa51199

Periodically, PPPoE and PPPoEoA configurations will experience ALIGN-3-TRACE tracebacks created by the PPPoE send PADS process.

These traceback messages occur randomly under configurations with PPPoE or PPPoEoA and do not appear to be related to any other negative behavior.

There are no known workarounds.

- CSCsa51333

An SSG subscriber loses connection to service.

When a user logs into an SSG service on the router with an idle timeout set for the connection, the connection is deactivated by SSG after a duration equal to the idle timeout even though the connection might have been active.

Workaround: Connection will not be cleared when there is activity if SSG service accounting is enabled and the accounting interval is less than the idle-timeout.

- CSCsa51394

Possible %ALIGN-3-SPURIOUS error messages.

This issue may occur when bringing up PPPoA sessions and, at the same, altering the configuration of the ATM interface over which these sessions are established.

Workaround: Avoid changing ATM config when bringing up sessions.

- CSCsa52472

On Cisco 10000 series routers, several drops are observed on a strict priority queue (PQ) when configured at high rate.

This issue has been observed on the following interfaces:

- STM4
- Gigabit Ethernet
- STM16

There are no known workarounds.

- CSCsa56748

On a subinterface, **ip flow ingress** command is used to enable netflow.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/swtch_r/swi_e1.htm#wp1101595

If netflow is enabled on one particular subinterface using **ip flow ingress**, then all the other subinterfaces get netflow enabled:

- Entries on the netflow cache for the other subinterfaces in sh ip cache flow is seen
- show ip flow interface only shows the interface where ingress netflow was configured

This issue is seen in a Cisco 10000 series router with PRE2 running Cisco IOS Release 12.3(7)X12.

There are no known workarounds.

- CSCsa57203

Configuring a “no pvc-in-range” on a VC range puts the VC in inactive state, even when there has never been any ATM traffic on the create on-demand VC. VC will become active once traffic is sent.

This issue occurs under the following condition:

```
!
vc-class atm default
  vbr-nrt 38 38
  dbs enable
  idle-timeout 60
  create on-demand
!
interface ATM5/0/0.1 multipoint
  atm pppatm passive
  range pvc 1/101 1/2052
  class-range default
  encapsulation aal5mux ppp Virtual-Templatel
!
```

When executing the command :

```
router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#interface ATM5/0/0.1 multipoint
router(config-subif)# range pvc 1/101 1/2052
router(config-if-atm-range)#no pvc-in-range 1/101
router(config-if-atm-range)^Z
AutoVC is enabled on the range
router#
```

The VC shows up in "show atm vc".

```
router#show atm vc
          VCD /
Avg/Min Burst
Interface Name          VPI  VCI  Type  Encaps  SC  Kbps  Kbps  Cells  Sts
5/0/0.1          8          1    101  PVC-A  MUX  VBR    38    38    50
INAC
router#
```

There are no known workarounds.

- CSCsa57216

When configuring a pvc-in-range, the router does not check for correct VPI/VCI pair. Omitting the VPI and entering VCI, a VC is created with VPI 0.

Another example is a bad VPI/VCI pair:

```
router(config-if-atm-range)#pvc-in-range 2/103
% Incomplete command.
```

This issue occur when configuring a pvc-in-range with invalid VPI or VCI.

There are no known workarounds.

- CSCsa58064

Attempts to create an ATM PVC on a point-to-point subinterface will fail if the PVC VPI/VCI had been configured on the subinterface previously.

A traceback will accompany the console log error and configuration error message.

To cause this problem to occur, create an ATM point-to-point subinterface, and configure a PVC on the subinterface. Remove the PVC and exit configuration mode.

Re-enter configuration mode and attempt to configure the PVC using the previously used VPI/VCI. The PVC will be created, but when exiting configuration mode, the PVC will be flagged as a second PVC where only one is allowed:

```
Jan 31 16:39:20.584: %ATM-3-FAILCREATEVC: ATM failed to create VC(VCD=8, VPI=100,
VCI=100) on
Interface ATM4/0/0, (Cause of the failure: Only one VCC allowed on a Point2Point
interface)
```

Workaround: Use ATM multipoint subinterfaces when possible. When point-to-point subinterfaces must be used, and a PVC needs to be removed and recreated, create a new ATM point-to-point subinterface using a new subinterface number.

- CSCsa58340

Upon entering the **police** command, the router reloads.

The reload occurs if the policy map being edited already contains the maximum number of classes that Cisco 10000 router supports, and the user attempts to add one more class with police.

Workaround: Avoid using policy maps that contain more classes than what Cisco 10000 supports null.

- CSCsa59200

IP QinQ currently not forwarded (dropped).

This issue occurs when sending IP to a QinQ subinterface.

There are no known workarounds.

- CSCsa59600

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCsa60348

Configuring service policy in the ingress direction on the virtual template does not work.

This issue occurs in PPPoEoVlan with service policy configured.

There are no known workarounds.

- CSCsa60613

The router with backup interface command configured under the gigabit ethernet interface will fail to perform the backup feature if shut/no shut the interface few times.

This issue is observed in Cisco IOS Release 12.3.

Workaround: Reload the router.

- CSCsa62420

With many active PPPoA PTA sessions terminated on a 10000 series router with PRE2 when the atm over-subscription-factor for a particular interface carrying these sessions is modified, some VCs will get stuck in the INACTIVE state, as seen in **show atm vc**.

This issue was seen with 5,000 PPPoA PTA sessions carrying 100M of bi-directional traffic. The problem did not affect L2TP tunnelled PPPoA or PPPoE sessions.

Workaround: To avoid this issue entirely shut the atm interface before changing the over-subscription-factor, otherwise a reset of the linecard or reload of the PRE2 clears the stuck VCs.

- CSCsa62475

The following message is logged:

```
%GENERAL-3-EREVENT: C10KSSG: Null c10k_turbo_acl for old out ACL
-Traceback= 60DBB7AC 60DBCE44 60DB670C 60DB6480 60DBB20C 60DB159C 60E09C68 60E09D4C
60E58434 60E585CC 608496AC 6085CD5C 6085CDD0 6084FD04 608559C8 60846C18
```

This issue is observed when a SSG user with a SSG output access-list defined in its RADIUS profile disconnect the PPPoX session.

Workaround: Define the ACL on the router and refer to it in the user profile instead of defining the ACEs directly in the user profile.

- CSCsa62939

PRE2 configured with APS may reload with a Bus error exception when show aps controller is issued in user mode or enable mode on a router running Cisco IOS Release 12.3(7)XI2.

This issue occurs on an APS configured on the PRE2.

There are no known workarounds. However, this command can be blocked (show aps controller) via tacacs.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

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 Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- 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 1 800 553-NETS (6387).

Documentation Feedback

You can send 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

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

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

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request 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 list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—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.

Severity 2 (S2)—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.

Severity 3 (S3)—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.

Severity 4 (S4)—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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *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 at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. 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/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0709R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.