



Release Notes for the Cisco 10000 Series Router for Cisco IOS Release 12.3(7)XI10a

First Published: August 14, 2007

Revised: September 24, 2008

These release notes provide information about Cisco IOS software Release 12.3(7)XI10a, which provides broadband aggregation, leased-line, and MPLS features for the Cisco 10000 series router.

Cisco IOS Release 12.3(7)XI10a is a maintenance release and there are no new features.

For a list of the software caveats that apply to Cisco IOS Release 12.3(7)XI10a, see the “[Caveats for Cisco IOS Release 12.3\(7\)XI10a](#)” section on page 15 and *Caveats for Cisco IOS Release 12.3T*. The caveats document is updated for each maintenance release and is located on [Cisco.com](#).

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.htm.

Cisco IOS Release 12.3(7)XI10a is based on the following releases:

- Cisco IOS Release 12.3T
- Cisco IOS Release 12.3(7)XI9

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/ios123/123relnt/xprn123/index.htm>



Corporate Headquarters:

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

© 2007 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\(7\)XI10a, page 3](#)
- [Enhancements for Alleviating High CPU Use, page 3](#)
- [Limitations and Restrictions, page 5](#)
- [Important Notes, page 12](#)
- [Caveats for Cisco IOS Release 12.3\(7\)XI10a, page 15](#)
- [Obtaining Documentation, page 85](#)

System Requirements

Cisco IOS Release 12.3(7)XI10a requires that the performance routing engine (PRE) is installed on the Cisco 10000 series router chassis [Part Number ESR-PRE2]. To verify which PRE is installed in the router, use the **show version** command.

Route Processor Redundancy Mode

When you upgrade or downgrade Cisco IOS software, the RPR mode used on the Cisco 10000 series router depends upon the Cisco IOS software currently running on the router and the Cisco IOS software to which you want to upgrade or downgrade. When you upgrade or downgrade from Cisco IOS Release 12.3(7)Xl to another Release 12.3(7)Xl, the RPR mode is always RPR+.

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 performance routing engine (PRE) is active and operational while the second PRE is in standby mode waiting for the active PRE to fail so that it can take over and maintain the operation of the router.
- In RPR+ mode—The standby PRE is fully initialized and configured, which shortens the time needed to switch over to the standby PRE.

Before You Upgrade 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 Performance Routing Engine Installation* at:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/hdwr/3971pr.htm>

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)XI10a

Cisco IOS Release 12.3(7)XI10a is a maintenance release and there are no new features.

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

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

Enhancements for Alleviating High CPU Use

Cisco IOS Release 12.3(7)XI10aa introduces the following enhancements to alleviate high CPU use:

- [Checking ARP Requests, page 3](#)
- [Policing and Dropping Encapsulation Diversions, page 4](#)

Checking ARP Requests

In Cisco IOS Release 12.3(7)XI9a, Release 12.3(7)XI10aa, and Release 12.2(28)SB7, an enhancement was added to enable the PXF to verify ARP packets before punting them to the route processor (RP). By performing ARP sanity checking for the interface on which the request was received, the PXF can send only valid ARP requests to the RP, thereby preventing the RP from becoming overloaded with ARP requests. This enhancement is useful when an ingress Ethernet interface is used for PPPoEoX aggregation.

In earlier releases, the PXF sends all incoming ARP requests to the RP for processing. However, not all ARP requests always require processing. Under some conditions, such as the following, ARP requests are considered invalid or unneeded:

- The ingress interface does not have an IP address configured
- The ingress interface receives an ARP request with a 13-target protocol address field that is not in the same subnet as the one configured on the interface.

For example, suppose the ingress interface is configured with the following IP address:

```
ip address 192.168.1.1 255.255.255.0
```

The interface then receives an ARP request for IP address 192.168.2.20 or 172.16.2.222. The PXF forwards the request to the RP without verifying it. Because these two addresses are not in the same subnet, the ARP request is invalid and the RP drops the request.

For more information, see the following topics:

- [Enabling and Disabling ARP Sanity Checking, page 4](#)
- [Restrictions for PXF ARP Sanity Checking, page 4](#)
- [Verifying Invalid ARP Requests, page 4](#)

Enabling and Disabling ARP Sanity Checking

To enable ARP sanity checking on all interfaces, enter the following hidden command in interface or subinterface mode:

```
pxf arp-sanity-check
```

Sometimes it is necessary to disable ARP sanity checking altogether (for example, for testing purposes). To temporarily disable ARP sanity checking on all interfaces, regardless of the individual interface configuration, enter the following command in global configuration mode:

```
ip pxf disable-arp-sanity
```



Note

These commands are available only when service internal is configured.

Restrictions for PXF ARP Sanity Checking

- When PXF ARP sanity checking is configured on an interface and the IP address or subnet mask of the interface changes, reconfigure the **pxf arp-sanity-check** command on the interface to save the new information to the PXF.
- When the PXF reloads, either by manually entering the **reload** command or due to a failure, the router does not automatically re-save PXF ARP sanity checking information to the PXF. After the PXF reloads, reconfigure the **pxf arp sanity check** command on all applicable interfaces.

Verifying Invalid ARP Requests

PXF statistics include the arp_req drop counter to identify the number of invalid ARP requests that the PXF identified and dropped. To view the PXF statistics, use the following command in privileged EXEC mode:

```
show pxf cpu stat drop
```

The following example shows sample output from the **show pxf cpu stat drop** command. In the example, the PXF identified and dropped 2105 invalid ARP request packets.

```
Router# show pxf cpu stat drop
FP drop statistics
           packets          bytes
generic           0             0
mpls_no_eos       0             0
fib_zero_dest     0             0
.....
ipm_replay_full   0             0
arp_req           2105          126300 <<<
bad_atm_arp       0             0
```

Policing and Dropping Encapsulation Diversions

In Cisco IOS Release 12.3(7)XI10a, an enhancement was introduced to police and drop encapsulation diversions (encap diverts).

All non-ARPA Ethernet packets are process-switched in Cisco IOS software and are, therefore, diverted to the RP. Some types of ARPA Ethernet packets are also diverted to the RP. If encap diverts increase rapidly, CPU use can become high. To alleviate this high CPU use, functionality was added to manage encap diverts before the PXF sends the packets to the RP.

The encap diverts enhancement adds a second route processor (RP) queue to enable rate-limited encap diverts to be tail dropped instead of being punted to the RP.

Configuring Encap Diverts Dropping

To allow encap diverts to be completely dropped before the PXF engine sends the packets to the RP, use the following command in global configuration mode:

```
ip pxf encap-divert drop
```

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)XI10a:

- [Binding a Service to Broadcast Interface, page 6](#)
- [Complete ID, page 6](#)
- [Controlling the Rate of Logging Messages, page 6](#)
- [DBS Extensions, page 6](#)
- [DNS Fault Tolerance, page 6](#)
- [DNS Redirection, page 6](#)
- [Frame Relay, page 7](#)
- [Full VAIs, page 7](#)
- [Half-Duplex Virtual Routing and Forwarding over Route Bridge Encapsulation, page 7](#)
- [IEEE 802.1Q-in-Q VLAN Tag Termination, page 7](#)
- [Layer 2 Tunnel Protocol Dialout, page 7](#)
- [PDSN Interworking, page 7](#)
- [Per Session Queuing and Shaping for PPPoE VLAN Using RADIUS, page 8](#)
- [PRE Network Management Ethernet Port, page 8](#)
- [Service Selection Gateway PTA MD, page 9](#)
- [RADIUS Proxy Enhancements for CHAP, page 9](#)
- [Range Command for Bind Statements, page 9](#)
- [Redundant Uplinks to the Same Service, page 9](#)
- [Scalability, page 10](#)
- [Service level ACLs, page 10](#)
- [SSG Auto Logoff, page 10](#)
- [SSG EAP Transparency, page 10](#)
- [SSG GRE, page 10](#)
- [SSG IOS NAT, page 10](#)
- [SSG L2TP, page 10](#)
- [SSG Prepaid, page 11](#)

- [Support for Classifying Hosts Based on IP Address, page 11](#)
- [Suppression of Unused Accounting Records, page 11](#)
- [Testing Performance of High-Speed Interfaces, page 11](#)
- [Unique Session ID, page 11](#)
- [VRF-Aware VPDN Tunnels, page 11](#)

Binding a Service to Broadcast Interface

Not supported.

Complete ID

Not supported.

Controlling the Rate of Logging Messages

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

We recommend that you configure the **logging rate-limit** command as follows. 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](#).

DBS Extensions

You must configure the AV pairs for both the high and low watermarks. Configuring only one of the AV pairs results in the watermark not being configured.

The Cisco 10000 series router only supports RADIUS Pull for automatically provisioned VCs and virtual path (VP) tunnels.

DNS Fault Tolerance

Not supported.

DNS Redirection

Not supported.

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.

Full VAIs

Full virtual access interfaces (VAIs) are not recommended for scaling because they consume significant memory and the router cannot scale to high session counts as advertised. However, there are times when full VAIs cannot be prevented. There are some known issues with regards to counters for full VAIs and if operation is considered incorrect, a case should be logged with the Technical Assistance Center (TAC).

Before opening a TAC case, refer to the CSCsc83107 caveat to make sure the issue is not the same.

Half-Duplex Virtual Routing and Forwarding over Route Bridge Encapsulation

Half-duplex virtual routing and forwarding (HDVRF) over route bridge encapsulation (RBE) is not supported.

IEEE 802.1Q-in-Q VLAN Tag Termination

PPPoEoQ-in-Q supports a maximum of 32,000 sessions per interface.

- IP over Q-in-Q (IPoQ-in-Q) supports a maximum of 16,000 IPoQ-in-Q subinterfaces per interface.
- IPoQ-in-Q supports a maximum of 448 outer VLAN IDs.
- Multiprotocol Label Switching (MPLS) is *not* supported on PPPoEoQ-in-Q and IPoQ-in-Q subinterfaces.

Layer 2 Ethernet over MPLS (EoMPLS) tunneling using the **xconnect** command on PPPoEoQ-in-Q and IPoQ-in-Q subinterfaces is **not** supported.

Layer 2 Tunnel Protocol Dialout

Layer 2 Tunnel Protocol (L2TP) dialout is not supported. SSG attempts to set up the tunnel, but does not set up the VRF for tunnel services. Therefore, traffic is not forwarded to the tunnel.

PDSN Interworking

Not supported.

Per Session Queuing and Shaping for PPPoE VLAN Using RADIUS

- The router does not support per session queuing and shaping for Layer 2 Access Concentrator (LAC) or L2TP Network Server (LNS) sessions. For LNS sessions, the router executes a session-level policy and any policies on the inbound and outbound interface.
- The QoS-related statistics available using the **show policy interface** command are not available using RADIUS.
- The router does not support using a virtual template interface to apply a service policy to a session.
- You can only apply per session queuing and shaping policies as output service policies. The router supports input service policies on sessions for other existing features, but not for per session queuing and shaping for PPPoE over VLAN using RADIUS.
- During periods of congestion, the router does not provide specific scheduling between the various PPPoE sessions. If the entire port becomes congested, the scheduling that results has the following effects:
 - The amount of bandwidth that each session receives of the entire port's capacity is not typically proportionally fair share.
 - The contribution of each class queue to the session's total bandwidth might not degrade proportionally.
- Including the ATM overhead in the shaping rate is not a user-configurable option. Whenever you apply a queuing service policy to a session, the router includes the ATM overhead in the queue and shape rates.
- The shaping rates on the router might be lower than the actual rate of the ATM link. This is because a networking device between the router and the subscriber's ATM link removes portions of the Ethernet frame (for example, a device removes the VLAN tags). The exact amount depends on the distribution of transmitted packet sizes.



Note The ATM overhead calculation includes the size of the Ethernet frame (the packet segment), including all VLAN tags.

- The router does not support the configuration of the policy map using RADIUS. You must use the modular QoS (MQC) command line interface (CLI) to configure the policy map on the router.

PRE Network Management Ethernet Port

Ensure that the Fast Ethernet, Network Management 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.

The interface should only be used for system management. Do not use this interface for operations such as Telnet and SNMP. The interface used for system management cannot terminate PPPoE or L2TP sessions.

Service Selection Gateway PTA MD

The Service Selection Gateway (SSG) PTA-MD is a form of Layer 2 switching. In the SSG implementation the host's PPP session is terminated by the access provider, but it may be logically associated with a particular service. Packets to and from the host are not routed normally but switched to and from the network to which the host is associated. This functionality is provided by designating the network-side interfaces as being associated with a service. The control plane then binds a host with a particular service based on service selection. This feature has evolved such that VRFs are used to ensure a host's packets are forwarded to and from the interface associated with the service to which they are bound.

If a network-side interface is designated as being associated with a service it is then bound to a VRF. Likewise, if a host subscribes to that same service it is also bound to that same VRF.

Packets to and from the host and to and from the network-side interface are routed within the same VRF. Therefore, packets to and from the host always traverse the service they have subscribed to first, regardless of the ultimate destination or original source.

A host cannot be connected to multiple services that are in different VRFs simultaneously.

RADIUS Proxy Enhancements for CHAP

Not supported.

Range Command for Bind Statements

To configure a non-PPP user as an SSG user, bind the interface as downlink or uplink by using the **ssg direction** command in subinterface configuration mode. The command syntax is:

```
ssg direction {uplink | downlink}
```

For example:

```
Router(config)# interface atm 5/0/1.15
Router(config-subif)# ssg direction downlink
Router(config-subif)# interface atm 5/0/1.16
Router(config-subif)# ssg direction uplink
```



Note

Note The **ssg direction** command also applies to range commands.

When you bind an interface to a direction, traffic is routed through SSG features and processing. If you do not bind an interface to a direction, the interface is a transparent passthrough interface and traffic is routed through normal Cisco IOS features processing.

Redundant Uplinks to the Same Service

Not supported.

Scalability

If you configure on-demand PVCs (individual and within a range) and PPP sessions, route processor (RP) CPU use can be 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 such as Dynamic Bandwidth Selection (DBS), ACLs, and service policies are enabled.

**Note**

Do not configure more than 1500 VCs under a multipoint interface. Exceeding this recommended limit can cause very high CPU use.

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 the call admission control **call admission limit** command.

Service level ACLs

Service ACLs cannot be applied to a connection. If this occurs, the connection remains active, but the ACLs have no effect.

SSG Auto Logoff

Use only one method of SSG auto logoff at a time: ARP ping or ICMP ping. ARP ping works only on hosts that have a MAC address.

SSG EAP Transparency

Not supported.

SSG GRE

You cannot configure GRE tunneling type interface as an SSG uplink interface.

SSG IOS NAT

Network address translation (NAT) functionality is not supported. This means that the router does not support concurrent access to multiple services for which the services, not the access provider, must assign the user's IP address.

SSG L2TP

Neither SSG acting as a PPP client proxy with LAC nor PPP session in L2TP getting SSG processing is supported.

SSG Prepaid

The SSG Prepaid feature has the following restrictions:

- Quotas are measured in seconds. You cannot change the unit of measure.
- The Cisco 10000 series router supports only time-based SSG Prepaid for a service connection.

Support for Classifying Hosts Based on IP Address

Not supported.

Suppression of Unused Accounting Records

Not supported.

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.



Note

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

Unique Session ID

Not supported.

VRF-Aware VPDN Tunnels

The Virtual Routing and Forwarding (VRF)-Aware VPDN Tunnels feature can only be used with Layer 2 Tunnel Protocol (L2TP) on the L2TP Access Concentrator (LAC). The reason is that the Cisco 10000 series router can only initiate tunnels in a VRF; it cannot terminate tunnels that arrive in a VRF. Therefore, this feature does not apply to the Cisco 10000 series router when the router is acting as the L2TP Network Server (LNS) because the Cisco 10000 series router, as the LNS, cannot terminate tunnels that arrive in a VRF.

For the multihop configuration, the ingress tunnel also needs to arrive in the global routing table, but the tunnel can be switched out into a VRF towards the final LNS destination.

Important Notes

This section provides important information about the following topics:

- [Configuring the `aaa new-model` Command](#), page 12
- [Enhancing Scalability of Per-User Configurations](#), page 12
- [Inserting a New Line Card](#), page 14
- [Provisioning for Scaling](#), page 14
- [Deferrals](#), page 15

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)X11 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 3-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 VSA` 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` VSA 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.

Each time 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.

Provisioning for Scaling

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

- [PPPoA Sessions with IP QoS Static Routes, page 14](#)
- [AAA Authentication on the NME Port, page 15](#)
- [Call Admission Control, page 15](#)

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

For more information, refer to the [Cisco 10000 Series Broadband Aggregation, Leased-Line, and MPLS 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 network management (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
```

Deferrals

Cisco IOS software images are subject to deferral. To determine if your software release is affected, we recommend that you view the deferral notices at:

<http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml>

Caveats for Cisco IOS Release 12.3(7)XI10a

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 section of this 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)XI10a.

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 is 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)XI10a

This section describes caveats that are open in Cisco IOS Release 12.3(7)XI10a.

CSCdk65707

After you issue the **no router bgp** command, the following error message may occur:

```
%SYS-2-CHUNKSIBLINGS: Attempted to destroy chunk with siblings, chunk...
```

There is no observable consequence on the router behavior.

There are no known workarounds.

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.

CSCdy19642

Performance counters under the VT1.5, T3, VT2 controllers for DS1/E1 are not updated/displayed correctly.

There is no known workaround.

CSCdy44066

When Single router-APS (SR-APS) is configured on 1-Port Channelized OC12/STM-4 line cards. If an APS switchover is executed, the controller state in the **show aps** command output shows as SignalFail.

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 Automatic Protection System (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 PPP Termination and Aggregation 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

ATM VP tunnel of 10Mb does not shape the traffic to the exact speed. There are violated cells on a connected ATM switch witch is policing the traffic.

Workaround: Lower the configured speed to 9999 Kbps to ensure the tunnel speed.

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.

CSCec66364

Cisco 7301 router takes too long to boot up. About 4 to 5 minutes.

There are no known workarounds.

CSCec80927

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

Workaround: Remove the **mtu** command from the virtual template configuration.

CSCec85628

Outgoing traffic is above VP speed on an 8-port E3/D3 ATM 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.

CSCed19311

When SSG ARP auto logoff feature is configured, certain users may not get logged off with the feature. User logging off using SESM or other means do not get affected.

Workaround: Configure ICMP ping logoff. Upgrade the code to the appropriate version.

CSCed20626

Exec process shows high CPU usage. 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 command: **dir device** command only for known good device names.

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: Use the **set** or **police** command to define a policy action.

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 VRFs, 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 use 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 using 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:

- 4,095 VRFs are configured on a router
- 500 eBGP sessions are established between the router (PE) and CE routers
- 540 VRF routes per VRF in the 500 VRFs that are running eBGP between PE and CE routers
- 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 OC-48 interface, PXF stops responding. This problem occurs when you allocate a small amount of bandwidth, and it only occurs on POS OC-48 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 OC-3 ATM line card. The reason it occurs in the OC-3 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 auto-VC, 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 1-port channelized OC-12 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 1-port channelized OC-12 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 a Super Frame (SF) that is configured on both ends. This problem occurs when you configure **T1 1 framing sf** under AU-3 on a 1 port channelized OC-12 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 OC-48 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 OC-48 interface as an output policy map.

Workaround: Use shaping instead of policing.

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 Cisco IOS Release 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 Cisco 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 and 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 OC-12 line card with SONET 768 encapsulation 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 does not 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 1-port channelized OC-12-SDH interface when running performance/scalability tests.

There are no known workarounds.

CSCee66066

BERT testing over a clear channel DS3 interface for the 1-port channelized OC-12 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 high CPU usage 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.

CSCee78728

Sometimes an ALIGN Traceback message displays for broadband PTA queue scaling after issuing a **microcode reload PXF** command.

There are no known workarounds.

CSCee78849

During a broadband PTA queue scaling traffic test, one-third of the subinterfaces' policy-map counters displayed a big number after issuing the **microcode reload pxf** command.

Workaround: Clear counter.

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.

CSCee83019

Malloc seen on reload 7300 when CDP is enabled.

Workaround: Disable CDP using the **no cdp run** command.

CSCee86091

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

There are no known workarounds.

CSCee88327

When the **ipv6 multicast-routing** command is configured on a router with 1000 sub-interfaces.

There are no known workarounds.

CSCee90904

In 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_ttcn_read: Invalid Address 3FC110A4
```

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

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 stops responding. 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.

CSCef08967

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

There are no known workarounds.

CSCef14249

When sending traffic with 1,024 byte large size packets over 120,000 queues with 80 percent OC-12 ATM 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 sub rates of the `8-port E3/DS3` line card.

There are no known workarounds.

CSCef17801

When configuring over 2,000 Frame-Relay DLCI interfaces on a 1-port channelized OC-12 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 Cisco 7301 NPPEG1 platforms.

Workaround: Disable the second CPU, however, this affects performance.

CSCef19259

If autovc is configured, traceback messages 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 using the policy map and/or the VC queue depth will improve the result.

CSCef24008

When using a 4-port channelized OC-3 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 high CPU usage 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 OC-12 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.

There are no known workarounds.

CSCef30873

The router can stop responding 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 line card 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 stop responding 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 OC-3 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.

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 using DBS. If the VC shaping rate is provisioned using 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 using 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 OC-3 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 OC-3 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 use 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.

CSCef80176

If a user has a vbr-nrt vc configured within a pvp and execute a **no vbr-nrt pcr scr mbs** command, the VC type will change to unshaped ubr and a traceback will be generated. Since only vbr-nrt VCs are supported within a vp tunnel, this operation will fail. This will lead to lingering VAI if there was a ppp session established on this VC.

The **clears counters** command tries to execute on the leftover VAI and causes the router to stop responding.

Workaround: Do the following:

- Change VBR-nrt parameters using the **vbr-nrt new_pcr new_scr new_mbs** command.
- Avoid deleting the VBR-nrt service configuration from a VC, which is configured within the PVP tunnel.

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.

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 high CPU usage 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 OC-12 ATM line card reloads multiple times during ATM card reset or boot up. This problem occurs with the latest segmentation and reassembly 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-port channelized OC-3 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 OC-12 ATM 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 was sent out in authentication requests, based on the configuration on the router was for the same. This problem occurred when the per-server group nas-port was configured on the Cisco 10000 series router in such a way that the nas-port value in all authentication requests were sent in format e string of 32 Is (VPI value of incoming session) and the accounting requests were sent in format e string of 32 Cs (VCI value of incoming session). However, on session bring-up, the authentication requests had a nas-port value representing the format e string value corresponding to 32 Cs, which was 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 4CHOC-3 line card on the Cisco 10000 series router platform. The T1 Multilink PPP member links are seen as up/down after a couple of MR-APS switchovers.

Workaround: Resetting the 4CHOC-3 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 using 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 4CHOC-3 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 use 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 Cisco Release 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.

There are no known workarounds.

CSCef94838

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

Workaround: Issue the **no ip domain server lookup** command.

CSCef95719

RP CPU use 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 use 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.

CSCef95814

Some of the ATM MIB objects return NULL. The objects are:

```
cAal5VccExtCompEnabled,
cAal5VccExtVoice,
cAal5VccExtInF5OamCells,
cAal5VccExtOutF5OamCells.
```

There are no known workarounds.

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 4CHOC-3 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 using the MR-APS Working and another using 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 failure 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 fails with the following error:

```
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

The OC-12 POS line card's receive interface counters are not accurate. The OC-12POS 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 load sharing 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)X11, 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 1-port channelized OC-12 or 4chstm1-1 line card.

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 subinterfacename** 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 use can be extremely high when bringing up PPPoA sessions when using I/F Policy Map AV Pairs.

There are no known workarounds.

CSCeg04026

Test Pattern is NULL for BERT pattern. It is seen in both 1-port channelized OC-12 and 4-port channelized OC-3 line cards

There are no known workarounds.

CSCeg04038

Ping fails across native VLAN1. The dot1q encapsulation is enabled between a Cisco 7500 and the first Cisco 10000 router, and between the second Cisco 10000 router and the first Cisco 12000 router. 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 use 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.

CSCeg05333

When pasting the config through the console port of the Cisco 10008 router the input stops once the command **service compress-config** is entered.

Workaround: Enter the config with the **service compress-config** command as the last command or paste the config using a VTY.

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 **show running-configuration** command stops working when traffic is sent at 141,000 packets/second on unopened VCs. 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)XI1 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 stop responding reporting a software forced crash (memory corruption). The problem occurs in Cisco IOS Release 12.3(7)XI1 and seems related to AAA.

There are no known workarounds.

CSCeg10588

On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI2, 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 high CPU usage.

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.

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.

There are no known workarounds.

CSCeg47701

Cisco 10000 series router can stop responding with bad block pointer error.

There are no known workarounds.

CSCeg56821

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

The test involves three subtests.

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

The first two subtests passed. Only the third subtest is failed. In the third subtest, invalid frame combinations are configured, and the link should be down once it is configured, but the link is up.

There are no known workarounds.

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.

CSCeg68959

Packet 5 expected to be diverted for clns_isis was not found

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.

CSCeg73739

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

There are no known workarounds.

CSCeg77405

Sometimes SAR Page Limitation of 510 pages cannot be achieved except if the Cisco 10000 series router is reloaded. The following error from the Line card is displayed 'config VC reassembler, channel descriptor allocation failure' And then only 256 VCs come up.

Workaround: Reloading the router.

CSCeg84454

When changing a policy-map for policy “COLA64” while I had 6000 PPPoE sessions active as a PTA, no traffic No Service policy applied. 10000 PPPoA session active as a LAC, no traffic; policy “COLA64” applied to all. 7500 RFC1483 active as PTA, no traffic; policy “COLA64” applied to all. When I tried to change the policy-map from the following and add a new class with priority, I lost the ACTIVE PRE to a software failure:

```
Router# show policy-map
  Policy Map COLA64
    Class class-default
      queue-limit 64
```

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

CSCeg86096

Policy map does not get deleted from Virtual Template.

There are no known workarounds.

CSCeg88253

Packet loss observed on the video queues.

There are no known workarounds.

CSCeh06824

Cisco 10000 series router: PRE2 PXF may unexpectedly reload with “PXF DMA TBB Length Error”.

There are no known workarounds.

CSCeh07013

Less than expected number of PPPOA users established when using a large multipoint configuration.

There are no known workarounds.

CSCeh08171

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

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

CSCeh20521

On Cisco 10000 routers using the Cisco 4 Port Channelized OC3 line card, when 300 or more VT T1 interfaces are configured with PPP encapsulation, some T1 links do not achieve full traffic line rate.

There are no known workarounds.

CSCeh24011

Broadband PTA PPPoE queue scaling with 31,500 sessions over 2 OC-12ATM 31,500 subinterfaces, only 29,000 sessions up after 30 minutes, CPU stays 70%.

There are no known workarounds.

CSCeh47234

ATM CLP bit set using the MQC does not get set on the ATM cells.

There are no known workarounds.

CSCeh50616

Traceback found in 5850E1 running stress with bulk analog and digital calls.

There are no known workarounds.

CSCeh54992

When Single router-APS (SR-APS) is configured on the Cisco 10000 series router 4 Port Channelized/STM1 line cards and traffic is flowing through all ports, traffic convergence takes more than 15 seconds if the active line card is reset.

There are no known workarounds.

CSCeh66971

When migrating to the Cisco IOS Release 12.2S image from Cisco IOS Release 12.3(7)XI, traceback messages appear.

There are no known workarounds.

CSCeh69194

Broadband PTA PPPoE over two OC-12 ATM 31.5000 subinterfaces with input police policy map in a virtual template, and an output three-queue policy map, about 7,000 PPPoE sessions up, and PTA show max class-map reached, out of memory error.

There are no known workarounds.

CSCeh70133

When flow bits manually set to the flow-off state for a particular VC, data leakage is seen out of that VCs queue

There are no known workarounds.

CSCeh70164

When flow bits manually set to the flow-off state for a particular VC, data leakage is seen out of that VCs queue

There are no known workarounds.

CSCeh70291

When you enter the **redundancy force-failover main-cpu** privileged EXEC command on a Cisco 10000 series router that is configured with two Performance Routing Engines (PREs), an automatic protection system (APS) switchover occurs on SONET line cards, which is incorrect behavior.

There are no known workarounds.

CSCeh97487

When configuring the OC-48 POS card on the Cisco 10000 series router, the router may see an unexpected exception causing the router to stop responding.

There are no known workarounds.

CSCei05997

Received packets per second (pps) is less than the expected pps per channel.

There are no known workarounds.

CSCei07064

GE input rate is abnormal large on Cisco 10000 series router with PRE2 12.3(7)XI3, the problem also can be seen on FE interface, ATM interface has no such problem.

There are no known workarounds.

CSCei13763

Feature request to have a passive pim interface on PIM. This is to include the virtual-template into the PIM process so that VAIs can be included in the MC process but not having to send hellos out.

There are no known workarounds.

CSCei34378

High CPU usage observed while running the managed Ins test.

There are no known workarounds.

CSCei38386

Traceback at barium enable, Ironbus restarted found while running WRED tests.

There are no known workarounds.

CSCei39771

Super ACLs are generating a high CPU after a reload.

Workaround: Configure MINI ACLs (8 ACE's max).

CSCei44933

The Cisco 10000 series router may encounter alignment errors when changing vc-class and QOS parameters on PVCs that host live sessions.

There are no known workarounds.

CSCei45309

When an F4 OAM is configured. The default VC's generated after configuring F4 OAM should be down if its configured on one side.

There are no known workarounds.

CSCei49797

Even though there's bidirectional traffic on the member link, the multilink bundle only shows an output traffic rate.

There are no known workarounds.

CSCei54595

An unframed E1 under SONET VT framing shows high throughput loss. This includes the 1-port channelized OC-12 and 4-port channelized OC-3 ATM line cards.

Workaround: An unframed E1 uses all 32 available channel groups, but a framed E1 can use up to 31 channels and reserve the last channel for framing bits. Since a framed E1 does not show the same performance loss, use the framed E1 line card with 31 channels.

CSCei57156

Spurious memory access found while configuring, when using the ODAP feature.

There are no known workarounds.

CSCei59146

When have ATM VCs with "queue-depth" configured under each VC, then establish PPPoA sessions with policies applied using RADIUS server, issuing **no dba enable** command under the VCs, causes all sessions to go down.

There are no known workarounds.

CSCei61754

Unable to bring up session with HDVRF feature.

There are no known workarounds.

CSCei67410

This is a rare race condition between the Virtual Exec/Exec process and processes that contend with the resources the **show sss session all** command uses. For this particular non-response, it was the session circuit memory that was in contention. The router accessed the memory after it was overwritten by another process.

There are no known workarounds.

CSCei69179

When l2tp session comes down, the disconnect reason is *carrier loss*. It should be lost service.

There are no known workarounds.

CSCei68924

The counter for the runts packets are not getting updated properly.

There are no known workarounds.

CSCei69146

When the **bandwidth** *kbps-bandwidth* command or the **bandwidth percent** *percentage* command and the **bandwidth remaining percent** *percentage* command are configured for a traffic class and the no bandwidth remaining percent command is entered to unconfigure the command, the **bandwidth** *kbps-bandwidth* command or the **bandwidth percent** *percentage* command is incorrectly removed from the running-configuration file rather than the **bandwidth remaining percent** *percentage* command.

Workaround: Unconfigure the **bandwidth remaining percent** *percentage* command for the second time and configure the **bandwidth** *kbps-bandwidth* or the **bandwidth percent** *percentage* command that was removed from the running-configuration file in the first unconfiguration of the **bandwidth remaining percent** *percentage* command.

CSCei70282

Unable to ping when session are brought up.

There are no known workarounds.

CSCei84735

When you issue the **show controller** command the output displayed indicates that the VT is up and it also shows an Invalid VT Status.

There are no known workarounds.

CSCei85614

Cisco 10000 series router running Cisco IOS Release 12-3(7)X15 when the command **redundancy force failover main-cpu** is issued %REDUNDANCY-3-CONFIG_SYNC: Active and Standby bulk configuration out of sync appears though configurations on both PREs is identical.

There are no known workarounds.

CSCei87171

When have 4093 qinq subinterfaces configured using one inner tag and 4094 outer tags per inner tag, establish pppoe sessions over the QinQ subinterfaces, traffic sent downstream direction gets lost on PTA side, where all traffic which was sent upstream direction is getting received.

There are no known workarounds.

CSCei87486

Traffic is not forwarded when a session flaps and comes back online.

There are no known workarounds.

CSCei91511

Customers using RFC1483 under multipoint ATM interfaces, uRPF does not work

Workaround: uRPF should be removed when using virtual template.

CSCei94381

When you unconfigure and then reconfigure a child policy map in a nested service policy using a different parameter for the police action (for example, burst parameter), the **police** command has no effect. This occurs when an assertion failure is seen while executing the **show policy-map interface** command. The output of the command does not display any police statistics.

Workaround: Unconfigure and configure the policy map under a Gigabit Ethernet subinterface

CSCei94474

QoS latency when using 1500 byte packets.

There are no known workarounds.

CSCei94642

Interface transition to down state after Performance Routing Engine switch over.

There are no known workarounds.

CSCej00113

PXF is observed to fail in post router check.

There are no known workarounds.

CSCej01828

The wrong I/P & O/P Packet count displays in the output of the **show interface** command for a full or base VAI, a sub-VAI, or a main interface.

There are no known workarounds.

CSCej11685

Seeing IRONBUS fault on 6-Port Channelized T3 line card on the Cisco 10000 series router. This is apparently seen when the card is not configured.

Workaround: Issue the command **hw-module slot x shut** to disable the card if it is not in use.

CSCej11073

Unable to configure SSG on a Cisco 10000 series router after a **no ssg enable force-cleanup** command has been executed.

There are no known workarounds.

CSCej21761

Test failed for post-router check for the fail.

There are no known workarounds.

CSCej25192

Exec process shows high CPU usage.

Workaround: Use a fewer number of small local IP pools rather than a single large local IP pool.

CSCej28207

Rounding of rates entered by user in Shape & Bandwidth policy action not informed to the user or reflected in **show run** command output.

There are no known workarounds.

CSCej28229

Packet drops in traffic class with WRED active is not accounted in SUB VAI statistics

There are no known workarounds.

CSCej28331

Unexpected packet drop in a traffic class.

There are no known workarounds.

CSCej32582

A Cisco 10000 series router experiences PXF failures with the following message:

```
stop responding reason 'PXF DMA TBB Length Error'
```

There are no known workarounds.

CSCej34315

Moving between releases which support and not support HH-CHT3 module causes the system to get into the above issue. In Cisco IOS Release 12.2(XI), the half-height channelized T3 module is not supported and hence the parser should reject the configuration, but it recognizes it as an unknown card type and it cannot be removed by using the **no card type** command.

Workaround: Remove the module from the slot.

CSCej48170

The output policy applied on some VCs, policed the traffic on a few VCs and did not police the traffic on rest of the VCs.

There are no known workarounds.

CSCej49129

Spurious memory access & error tracebacks while bringing down the session.

Do not config the unsupported config.

CSCej49351

On a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI6, subscribers using the PPPoE TAG feature wait for more than 20 seconds before they get connected. After further troubleshooting, it is determined that the Cisco 10000 series router sends PPPoE PADS and the first LCP request at the same time. Sometimes LCP REQ gets received before the PPPoE PADS. For that reason the CPE discards the LCP REQ packet without sending any LCP packet back to the Cisco 10000 series router, which waits for 20 seconds (**ppp timeout retry default** command) before sending that LCP REQ again.

Workaround: Use the **ppp timeout retry** command in the Virtual Template to reduce the timeout retry.

CSCej56912

Error traceback at **c10k_get_aggregated_queue_raw_counters** command is sent to the server console every 10 seconds.

There are no known workarounds.

CSCej60620

Downloading PCR/SCR values that are negative or alpha (not numerical) causes an issue with any sessions that follow that particular radius download of values. Once the VC is destroyed and recreated (along with the interface) the PRE stops responding with a bus error.

Workaround: Verify that PCR/SCR, weights, and watermarks are valid integers and not greater than the PCR/SCR of the interface.

CSCej69414

Tests failing while bringing 31500 session with 4 policy queues configured.

There are no known workarounds.

CSCej73450

The Cisco 10000 series router software is looking into the PPPoE hash table and sessions.
There is no known workaround.

CSCej75389

On a mutlilink line card all interfaces switch to the protect card after a router processor switch over.
There are no known workarounds.

CSCej75472

Traffic loss through router configured as both Working and Protect routers.
There are no known workarounds.

CSCej75851

When trying to verify server group failover and deadtime for a per-VRF AAA configuration, the ACCT-START and ACCT-STOP are not sent to the active private-server host.
There are no known workarounds.

CSCej76102

Cisco 10000 series router may encounter lots of traceback and error messages while running configuration of PPPoEoA and DBS (Dynamic Subscriber Bandwidth Selection) and moderate downstream traffic. As a result, some PPPoEoA sessions may fail. The following is a sample of the error message that displays:

```
C10K_QUEUE_CFG_GENERAL-2-EREVENT
Cannot create default queues
```

There are no known workarounds.

CSCej76827

Traceback observed when the **ipc_send_rpc_blocked** command failed.
There are no known workarounds.

CSCej76986

The dsx3LineType does not match the CLI-obtained value.
There are no known workarounds.

CSCej76995

Idle timeout brings the auto-VC down in the presence of a PPPoE session.
There are no known workarounds.

CSCej77417

Unable to scale up to 32k sessions for PPPoA qos_input_output_rate_limiting.
There are no known workarounds.

CSCej77972

Traffic is lost as the adjacency table on the client, LAC and LNS are not consistent.
There are no known workarounds.

CSCej85614

PRE stops responding while testing POD functionality.

There are no known workarounds.

CSCej85707

PRE stops responding while simultaneously accessing configuration.

There are no known workarounds.

CSCej85905

Traffic rate reduction after manual Multi Router Automatic Protection Switching (MRAPS) switch over.

There are no known workarounds.

CSCej89551

Queue depth not properly set for class with WRED configuration.

Workaround: Use queue-limit action to set the queue depth instead of relying on the default depth of the WRED class.

CSCek00691

The Cisco 10000 series router does not support the use of Turbo access lists (ACLs) with SSG sessions. Instead, use mini-ACLs, which consist of a maximum of 8 ACL rules (statements). Any rules that permit traffic by specifying Layer 4 matching criteria count as two rules.

Workaround: Use mini-ACLs.

CSCek01900

The **show policy-map interface subvai** command displays unexpected statistics for a few sessions.

Workaround: Execute the **clear counter** command after reloading the Microcode.

CSCek02167

Random drops and Max threshold drops are summed and shown under default value (zero here) in WRED stats than against individual values.

There are no known workarounds.

CSCek04267

Unable to delete PVC messages during online removal and insertion of an ATM line card.

There are no known workarounds.

CSCek04301

Serial interfaces report throughput statistics with values that are impossible to attain.

There is no known workaround.

CSCek11664

A forwarded packet may be lost on a PPPoE session on a Cisco 10000 series router.

There are no known workarounds.

CSCek17507

The router creates virtual access interfaces (VAIs) before verifying that the sessions are still valid. The router needs to implement the vtemplate-cancel API before creating VAIs.

There are no known workarounds.

CSCek29312

Traceback and error messages occur when PPPoA sessions are brought up.

Workaround: If CPU use is very high (99 percent), wait until the CPU use goes down.

CSCek35147

Buffer leak observed on the far-end Cisco 10000 series router upon switchover under bi-directional traffic conditions on the near-end redundant Cisco 10000 series router.

There are no known workarounds.

CSCek41726

The Cisco 10000 series router memory can be reduced to a very low value if the Service Selection Gateway (SSG) accounting interval is enabled. Also, memory fragmentation and memory leak is observed.

There are no known workarounds.

CSCek53052

Issuing the **l2tp tunnel timeout no-session never** command generates an invalid configuration, which results in the router ignoring the command after rebooting. The following sample configuration shows the invalid configuration:

```
Router# l2tp tunnel timeout no-session never

vpdn-group 1
 accept-dialin
 protocol l2tp
 virtual-template 1
 terminate-from hostname sp_lac
 local name lns
 no l2tp tunnel authentication
 l2tp tunnel password 7 02050D480809
 l2tp tunnel no-session-timeout -2 <----- invalid configuration option
```

This problem occurs when configuring L2TP tunnels.

Workaround: After rebooting, reconfigure the **l2tp tunnel timeout no-session never** command. Depending on network usage, setting the no-session timeout to a large value might also fix the problem.

CSCek59605

A process_suspend() does not work as expected, causing the router to show high CPU usage.

Workaround: Format the slot devices and quit the session.

CSCin65670

During Multiplex Section Protection (MSP), the cutover traffic received rate is less than the transmit rate.

There are no known workarounds.

CSCin68641

In Cisco IOS Release 12.3(4)T3, when trying to configure a VPDN-group for PPPoE after removing the previously configured **bba-group** command for PPPoE, the **protocol** command in the VPDN accept-dialin configuration mode does not allow the PPPoE option.

Workaround: Before removing the **bba-group** command, remove all references to the group. This requires the user to manually remove, from all interface and PVC specifications, either the protocol or encapsulation statements that reference the BBA group to be deleted. Please note it is currently not enough to only remove the interface (or subinterface) or PVC specification—the subordinately defined BBA group references must also be specifically and completely removed.

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-recod authentication failure** command is configured.

Workaround: Disable **aaa accounting send stop-record authentication failure** command if it's not needed.

CSCin77394

Throughput is less for packet size 64,128 and 256 bytes. For higher bytes like 512, 1024 and 1472 works fine.

There are no known workarounds.

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.

CSCin93792

UUT stops responding when vpn service is configured with domain name longer than 210 characters, on a router when you enter the **vpn service domain name** command.

There are no known workarounds.

CSCin99774

Unauthenticated users are able to access any active service of logged-in users on the Cisco 10000 series router.

There is no known workaround.

CSCin99937

Connection set up fails at the tunnel-service hardware on the Cisco 10000 series router.

There is no known workaround.

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.

There are no known workarounds.

CSCsa51199

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

There are no known workarounds.

CSCsa54608

The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

Only devices running certain versions of Cisco IOS are affected.

Cisco has made free software available to address this vulnerability. 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-20050907-auth_proxy.shtml

CSCsa57074

It can take up to 70 seconds between accepting two successive **test PPPoE** commands.

There are no known workarounds.

CSCsa58168

Packets passing through a policed priority queue (PQ) on the LAC are dropped.

Workaround: Increasing the policed bps rate within the PQ lessen the drops somewhat, but do not alleviate the problem.

CSCsa60348

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

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.

CSCsa70255

The router stops responding in policy-map update counter.

Workaround: Increasing the shut/no shut time interval from 2 minutes to 4 minutes in script solves the problem.

CSCsa72607

Cisco 10000 series router acting as a PTA stops responding with 10,000 sessions and 14 tunnels.

There are no known workarounds.

CSCsa73827

Spurious access seen when booting with SSG configuration may be observed

There are no known workarounds.

CSCsa74244

After upgrade from 12.2 (16) BX3 to 12.3 (7) XI2 on Cisco 10000 series router, you get about 7% of L2TP tunnel in wt-sss state.

There are no known workarounds.

CSCsa81233

On Cisco 10000 router, 4OC-3ATM card disconnected all users and showed connecting sessions stuck in LCP. All interfaces on the card don't increase output packets and PVCs go down if OAM management is enabled.

Workaround: Reset ATM card.

CSCsa87620

The output of the command **SH PXF CPU QUEUE ATM** shows incorrect. Each of the ATM regular data packets, and one for high priority packets.

There are no known workarounds.

CSCsa90094

A Cisco 10000 router running 12.3(7)XI3a code may display the incorrect value in the "Total subscriber rate" field in the output of the **show controller atm x/y/z** command.

Workaround: The issue appears to be cosmetic with no adverse effects.

CSCsa99913

ALIGN-3-CORRECT and ALIGN-3-TRACE seen on a Cisco 10000 series router running the 123_7_xi2a throttle versions 050412 and 050227.

There are no known workarounds.

CSCsb08395

Feature Request to enhance the present show command **show atm class-links VPI/VCI** to include the vc-class name that is applied to the vc.

There are no known workarounds.

CSCsb09341

Policy-map policing is not properly allowing full data rate when the time is outside of the policed time-range.

Workaround: Use the transmit option instead of the drop option in the **police** command.

CSCsb12507

PPP/MLPPP is not behaving properly under mis-matched keepalives and no-keepalives on the serial interfaces of both ends

There are no known workarounds.

CSCsb13188

After the primary Radius server was turned off the authentication request were send to the secondary Radius server, but the server still showed as UP.

Workaround: The issue appears to be cosmetic with no adverse effects.

CSCsb17545

A PXF fails with a Cobalt Error being flagged. When two IP fragments arrive on an LFI-type link that are destined for the Cisco 10000 series router, the rare possibility exists (depending on the number of the LFI fragments received) that an error will be hit.

There are no known workarounds.

CSCsb23485

When doing a tag swap or push, a **set exp** command in an input policy map is ignored. The specified EXP value is not written to the newly imposed tags, nor can output QoS match on the new EXP value.

There are no known workarounds.

CSCsb26615

The following messages appear:

```
ATM-3-FAILREMOVEVC: ATM failed to remove VC message
%C10K-3-LC_ERR: Slot[1/0] 4OC-3ATM-1 SAR: modify VC, invalid channel handle 0x0699on port
2 every 15 minute
```

There are no known workarounds.

CSCsb32588

PPP sessions may fail to establish on a VC.

Unconfigure the VC class, wait a couple of seconds and configure it again.

CSCsb44601

Traceback messages displayed during downgrade from Cisco IOS Release 12.2 SBB to 12.3(7)XI5.

There are no known workarounds.

CSCsb44698

Traceback messages during downgrade from 12.2(27)SBB to 12.3(7)XI5.

There are no known workarounds.

CSCsb53216

Traffic is forwarded across a GE sub-if when the sub-if is shutdown in a PPPoE configuration.

There are no known workarounds.

CSCsb53950

The interface counters on the main GE interface are incorrect when using PPPoE over VLAN configuration. This affects both the CLI and SNMP counters. This condition is not seen with IP only traffic.

There are no known workarounds.

CSCsb55174

Running the interim image based on Cisco IOS Release 12.3(07)XI., the router shows the following alignment errors:

```
May 26 16:57:28.059 METDST: %ALIGN-3-CORRECT: Alignment correction made at 0x60DEB8B8
reading 0xD0D0D09
May 26 16:57:28.059 METDST: %ALIGN-3-TRACE: -Traceback= 60DEB8B8 6034D6F8 6034D8F0
603476EC 60349D68 60339138 60C30224 60C39F14
May 26 16:57:28.059 METDST: %ALIGN-3-CORRECT: Alignment correction made at 0x60DEB8D4
reading 0xD0D0D09
May 26 16:57:28.059 METDST: %ALIGN-3-TRACE: -Traceback= 60DEB8D4 6034D6F8 6034D8F0
603476EC 60349D68 60339138 60C30224 60C39F14
May 26 16:57:28.059 METDST: %ALIGN-3-CORRECT: Alignment correction made at 0x60DEB904
reading 0xD0D0D09
May 26 16:57:28.059 METDST: %ALIGN-3-TRACE: -Traceback= 60DEB904 6034D6F8 6034D8F0
603476EC 60349D68 60339138 60C30224 60C39F14
```

Decoding them, all point to:

```
ssg_aaa_acct_get_component_specific_dynamic_attrs__FPvU1
```

There are no known workarounds.

CSCsb55246

PXF fails with DMA length error.

There are no known workarounds.

CSCsb55621

On a Cisco 10000 series router, the command **ip idle-group** does not work in conjunction with the command **ppp timeout idle**. The idle time will expire regardless of whether or not any traffic is present to reset the timer.

Workaround: Use the idle timer without the idle-group function.

CSCsb59396

Cisco 10000 series router running a 12.3(7)XI2a-based image experienced a non-response at the following function: GetPrepaidIdleTime__16ConnectionObject SSG related.

There are no known workarounds.

CSCsb61775

High CPU(IP RIB Update) and traffic drop may be experienced during VRF deletion.

There are no known workarounds.

CSCsb62479

A Cisco 10008 router acting as LAC and also performing PTA for PPPoA sessions received the following message on the console or in the log file:

```
Assertion failure in /view/BLD-v123_7_xi3a1_throttle.V123_7_XI3C/vob/ios.sys4/sys/obj-4k-
c10k/./toaster/c10k_rp/c10k_qos.c:abs_priority_notification_handler() (4649) Expression
'service_policy_local' = 0x0
```

There does not appear to be any impact to traffic or sessions on the router.

Workaround: This problem required many modifications to be occurring simultaneously on the box and a reasonably high level of traffic. The workaround therefore is to reduce the number of service-policy configuration changes made per second. Avoiding executing the **show policy-map interface** command while removing a service-policy should also avoid this problem. These messages did not appear to have a detrimental affect on the sessions or traffic.

CSCsb64984

The following messages appear:

```
%ATM-3-FAILREMOVEVC: ATM failed to remove VC.
%ATM-3-OUT_OF_VCDS and %ATM-3-FAILREMOVEVC
```

There are no known workarounds.

CSCsb66252

When running multiple instances of the **show pxf cpu queue ATM x/y/z** command while deleting or adding service policies and overwriting the VC class on many PVCs, the Cisco 10000 series router might stop responding with a bus error.

There are no known workarounds.

CSCsb68306

PRE2 PXF stops responding with PXF DMA TBB Length Error.

There are no known workarounds.

CSCsb78535

A Cisco 10000 router might show the following log message:

```
c10k_l2tp_hw_session_open: not able to retrieve vcci
```

There are no known workarounds.

CSCsb79060

Random T1s in a channelized OC-3 line card are sending LOF. The result is that the T1 is down/down.

Workaround: Reloading the line card using the **hw-module slot x reset** command restores normal operation.

CSCsb79666

If a new Cisco 10000 series router 6-port OC-3 line card is inserted into a Cisco 10000 router and then HDLC encapsulation is configured, the POS interface does not send out any keepalive packets. The **show interface** command does not display the `keepalive set` line.

There are no known workarounds.

CSCsb82118

The **clear ip route download** command deletes the routes first causing a withdraw in BGP.

There are no known workarounds.

CSCsb87975

Traceback on microcode reload with three 1000 PPPoEoQinQ sessions up.

There are no known workarounds.

CSCsb88950

When terminating PPPoE clients on a Cisco 10000 router running 12.3(7)XI5, clients from some vlans are unable to login to the network.

Workaround: Reload the router. Additionally, removing and re-entering the subinterface configuration for the specific VLAN may resolve the issue.

CSCsb91234

The **show bgp** command replication cause alignment error.

There are no known workarounds.

CSCsb91550

Tracebacks seen when microcode reload is performed, and Exec process shows high CPU usage.

There are no known workarounds.

CSCsb93384

General Queue event and alignment errors when assigning a new PCR value through DBS to sUBR VCs. No observable function loss with these errors was found during testing.

There are no known workarounds.

CSCsb94195

A traceback occurs when establishing PPPOA/PPPOEOA sessions with an associated output service-policy applied.

There are no known workarounds.

CSCsb96615

Spurious memory access at **c10k_netflow_sw_setup_ingress** command. When a PPPoEoA session comes up.

There are no known workarounds.

CSCsb97682

The PXF on a Cisco 10008 router might not respond and the following message displays:

```
C10KEVENTMGR-1-MAJOR_FAULT: PXF DMA TBB Length Error, Restarting PXF
```

There are no known workarounds.

CSCsc00745

An MIB object needs to be defined to obtain the packet buffer memory information from the PXF/RP that is visible with the command **sh pxf cpu queue sum**

There are no known workarounds.

CSCsc04234

Error traceback at **c10k_get_aggregated_queue_raw_counters** is thrown to the server console every 10 seconds.

There are no known workarounds.

CSCsc05136

The PRE2 PXF does not respond and the following error displays:

```
PXF DMA TBB Length Error
```

There are no known workarounds.

CSCsc08516

When setting a tap of more than a 32 bit mask and having both source and destination in a packet belonging to that same subnet, the following error message displays:

```
Sep 30 06:45:35.727: %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=63EA6E34, count=0
```

Workaround: Make the address of the target identity a /32 bit mask.

CSCsc08590

Exec process shows high CPU usage messages for ACL and SNMP processing on a system with many sessions and a ubiquitous (to/from 0.0.0.0/0) tap.

Workaround: Make the tap more specific if possible.

CSCsc09704

CEF scanner is causing high CPU usage.

There are no known workarounds.

CSCsc11454

Traceback messages (such as the following) occur during a downgrade from Cisco IOS software image 12.2(27-7.29)SBB1 to Release 12(3)7XI6.

```
00:02:50: %IPC-4-NOPORT: Port Not Found. C0000 --> 10016, Index:3, Seq: 678, flags: 0, size: 276
```

There are no known workarounds.

CSCsc12503

Memory fragmentation occurring. Possibly related to AAA and/or SNMP when virtual template SNMP is configured.

There are no known workarounds.

CSCsc12535

Non-idle users are disconnected after an idle-timeout occurs.

There are no known workarounds.

CSCsc17278

A VRF prefix that has two routes to a destination (load balanced) may send all the traffic through a single interface. PXF CEF information shows a single path. The information in the **show ip cef vrf** command and the **show pxf cpu cef vrf** command is not consistent.

There are no known workarounds.

CSCsc19588

Fast Ethernet interface flapping after issuing the **enable cdp** command on an interface.

There are no known workarounds.

CSCsc22473

A Cisco 10000 series router stops responding due to the **turbo_acl_process** command when running Cisco IOS Release 12.3(7)XI2b.

There are no known workarounds.

CSCsc22692

The amount of free processor memory decreases every day. The PPP events process is slowly taking all the memory without freeing memory. This happens on a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI4 configured with SSG.

Workaround: Regularly scheduled reload of the router will release all the memory allocated by the PPP Events process.

CSCsc23842

Unable to generate full core dump on standby PRE.

There are no known workarounds.

CSCsc27090

Need support **show atm vc** command on Cisco 10000 series router.

There are no known workarounds.

CSCsc29077

Stateful switchovers to the redundant RP can take longer after the configuration of the interface encapsulation on the channelized OC-3 or OC-12 line cards have changed. After the cutover it can take 60 seconds or longer for full traffic to resume.

There are no known workarounds.

CSCsc29185

Traffic is interrupted for approximately 120 seconds during an RPR+ switchover.

There are no known workarounds.

CSCsc32974

PRE stops responding and indicates:

```
%PXF-2-FAULT:
```

There are no known workarounds.

CSCsc33012

The following message displays:

```
%ALIGN-3-CORRECT: Alignment correction made at 0x604D836C reading 0xB0D0B0D==> A possible memory corruption
```

There are no known workarounds.

CSCsc33334

PRE stops responding while collecting some policy map related counters.

There are no known workarounds.

CSCsc33381

PPP traceback messages occur when applying per-user attributes.

Workaround: The system recovers by itself.

CSCsc37413

When sending traffic through the PQ then Netflow does not record any flow data. This is happening only when Netflow is configured on the Multilink interface. The serial member links are not set to collect Netflow.

Workaround: Configure Netflow on both the multilink and its member links for Netflow to work for PQ traffic.

CSCsc37455

Spurious memory access could be seen when using PPPoE.

There are no known workarounds.

CSCsc39166

Burst session create/delete with high CPU usage causes the active PRE2 switchover on c10k_clr_queue_enqprep_tcm.

There are no known workarounds.

CSCsc39467

When running MR-APS between Cisco 10000 series routers in an EvDO environment. There is a T1 active on each Cisco 10000 series router going out to a Base Transceiver Station (BTS). If a T1 is active over each Cisco 10000 series router, the BTS reloads due to losing communications with the Radio Node Controller (RNC). The RNC resides on the Cisco 10000 series router GE LAN. During this time, traceroutes from the RNC show a loop between the two Cisco 10000 series routers over redundant VLANs between them and used for PGP and OSPF.

Workaround: Downgrades back to XI or disable PXF.

CSCsc41134

Cisco 10000 series router stops responding at **pim** commands.

There are no known workarounds.

CSCsc41290

When mixing the route of VRF wcm008 and VRF wcm077 by route-target import and export in PE1, but after remove the vrf wcm077 in PE1, it was found that the vpnv4 bgp entry still has the route-target of the wcm077, although the VRF wcm077 in PE1 had been removed.

There are no known workarounds.

CSCsc42515

Dead memory and corrupted dead process name generated during high CPU use.

There are no known workarounds.

CSCsc42659

On-demand VC becomes stuck after a PRE2 switchover if the **set atm idle-timeout** command is set to 1. There are no known workarounds.

CSCsc42985

Cisco 10000 series router, running Cisco IOS Release 12.3(7)XI5, might stop responding when you change the *percentage* value in the **police percent** command of a service-policy.

There are no known workarounds.

CSCsc43635

Cisco 10000 series router stops responding at **adjacency_add_for_atmvc_all** command.

There are no known workarounds.

CSCsc44182

When a time based ACL is used as a match criteria in a match all scenario, the order of when this ACL is matched/used affects the operation of the class-map match statement in a policy-map.

There are no known workarounds.

CSCsc44275

Route processor stops responding because of memory corruption caused by PPPoE packet corruption.

There are no known workarounds.

CSCsc47934

Cisco 10000 series router line VTY is still busy after issuing the **clear line vty** command.

There are no known workarounds.

CSCsc48355

Cisco IOS fails when you change the policy map or queue depth (or both) repeatedly for ATM PVCs after a switchover.

Workaround: Do not repeatedly change the policy map or queue depth (or both).

CSCsc49599

After clearing PPPoE sessions, the sessions are not seen anymore in the output of the **show pppoe summary** command as expected, but they are seen in the output of the **show sss sessions** command.

There are no known workarounds.

CSCsc51423

Both multirouter automatic protection system (MR-APS) ports report Active.

Workaround: Force an MR-APS cutover using the **aps force** command, or configure the **shutdown** or **no shutdown** command on one of the MR-APS interfaces.

CSCsc51520

Mismatch between Cisco IOS software and the ATM line card as to how many VCs are created.

There are no known workarounds.

CSCsc51710

Packet loss caused by shutting down ATM subinterface with RBE, and static routes pointing to subinterfaces.

Workaround: Remove static route referencing shutdown interface.

CSCsc54396

A Cisco 10008 PRE2 may stop responding due to memory corruption if packet handles are depleted.

Workaround: Do not configure more interfaces than those allowed by the system (avoiding using more than the 4096 packets handles). When the limit is being reached a warning message is shown to the user. Do not configure more queueing subscriber/interfaces at that point.

CSCsc54539

Security ACLs with more than eight ACL entries stop working and either permit all traffic or drop all traffic on a Cisco 10000 series router.

Workaround: Never use an ACL in a class map that is also used for security.

CSCsc56263

A Cisco 10000 series router may experience multiple PXF non-responses shortly after configuring Multicast using **ip multicast-routing** and **ip pim sparse-mode** commands.

There are no known workarounds.

CSCsc58675

During an active PRE2 switchover, the router fails at atm_get_idle_timeout_params.

There are no known workarounds.

CSCsc60017

After a PRE2 switchover, configuring the shutdown or no shutdown command causes an on-demand range VC to become inactive (INAC).

There are no known workarounds.

CSCsc61178

The **show redundancy state** and **show redundancy** commands on Cisco 10000 series routers running Cisco IOS Release 12.3(7)XI6 with two PREs and RPR+ configured does not clearly display that RPR+ is the redundancy mode.

There are no known workarounds.

CSCsc61211

ATM PVC failure due to no enough bandwidth upon APS switchover

Workaround: Reload the Cisco 10000 series router and all the PVCs will come back OK.

CSCsc61988

Call admission needs improvement.

Workaround: Enhance the call admission control (CAC) feature by configuring the CAC, instead of the CPU, to work on the number of incoming calls with a low and high watermark.

CSCsc63969

On the Cisco 10000 series router, a Lawful Intercept fragmented packet (2nd fragment) is not tapped. There are no known workarounds.

CSCsc65489

System stops responding in DMA stats collector. There are no known workarounds.

CSCsc65624

When the system is on high CPU use, resetting the ATM line card might cause the state of the static VC to become inactive (INAC). There are no known workarounds.

CSCsc65655

System non-response observed in Micro_get_block. There are no known workarounds.

CSCsc66947

In a multirouter-APS (MR-APS) pair, shutting down the Working ATM interface causes the router containing the Protect ATM interface to hang.

Workaround: Do not shutdown the Working OC12ATM interface, which causes an APS switchover to the Protect OC-12 ATM interface.

CSCsc69861

The following message appears:

```
Service Selection Gateway: Send VSA 9.2 for IPoQinQ, 9.2 for PPPoE
```

There are no known workarounds.

CSCsc69892

The following message appears:

```
Service Selection Gateway: Add VSA 9.2 for IPoQinQ users, VSA 9.1 for PPPoE users
```

There are no known workarounds.

CSCsc70976

A Cisco 10000 series router may reload with a Software Forced stop operation. There are no known workarounds.

CSCsc74431

Output rate counters in virtual access interface are wrong:

```
Virtual-Access1405 is up, line protocol is up,
 30 second input rate 0 bits/sec, 0 packets/sec
 30 second output rate 63007000 bits/sec, 8282905 packets/sec
 240436 packets input, 24183649 bytes, 0 no buffer
 421265 packets output, 625628031 bytes, 0 underruns
```

There are no known workarounds.

CSCsc74452

When performing a downgrade from IOS 12.3(7)X17 and above to 12.3(7)X13 Spurious Accesses may be reported.

There are no known workarounds.

CSCsc75789

Cisco SONET controller does not report active AIS alarm on the Channelized STM1 line card.

There are no known workarounds.

CSCsc75805

Cisco 10000 Channelized STM1 line card APS shows the wrong Tx K2 value.

There are no known workarounds.

CSCsc75903

Show policy map for virtual-access interface / subinterface, does not increase the policer counters in a Cisco 10000 series router.

There are no known workarounds.

CSCsc81876

A Cisco 10000 router may stop responding, hang or report CPU HOG after issuing the **show pxf interface** command without specifying an interface.

Workaround: Always specify an interface when using this command: **show pxf interface *interface***

CSCsc83080

Both rate and traffic counters do not display correctly on a full VAI.

There are no known workarounds.

CSCsc83269

PIX CEF values change causing packet loss.

Workaround: Shutdown the redundant path.

CSCsd25119

The **show policy-map** command displays incorrect counter information for the OC-48 ATM line card. This occurs when the router is policing outbound traffic on the OC-48.

There is no known workaround.

CSCsd36790

A traceback message displays on the far-end Cisco 10000 series router due to a possible PRE switchover event on the near-end Cisco 10000 series router.

There are no known workarounds.

CSCsd53421

Packet drops in traffic class with WRED active is not accounted in sub VAI statistics.

There are no known workarounds.

CSCsd77256

Multirouter-automatic protection switching (MR-APS) active is switched from the Protect router to the Working router while PRE2 cutover is performed from slot B to slot A. This behavior was observed when APS is configured with 1-Port Channelized OC-12 line cards with MLPP.

There are no known workarounds.

CSCse09410

The Cisco 10000 series router rate counter does not work as expected on Gigabit Ethernet interfaces.

There is no known workaround.

CSCse11991

The Cisco 10000 series router fails in MGDTIMER Process=ATM ARP INPUT.

There is no known workaround.

CSCse19234

PVC creation under VP should fail when usingubr+ from vc-class.

There is no known workaround.

CSCse32498

Traceback messages appear when doing a high availability check on the 4-port channelized STM-1 line card (for example, (HA-4chhtml-vpn_basic_ospf_bgp.router_check)).

There is no known workaround.

CSCse34117

Bandwidth use is low on scaled environments. If you configure large numbers of multilinks with traffic consisting of smaller packets, packet drops occur, link use is very low, and traceback messages and first-in-first-out (FIFO) errors might also occur.

There is no known workaround.

CSCse44271

The Cisco 10000 routers ignore some errors and also experience cosmetic input errors.

There is no known workaround.

CSCse53387

If there are multiple PPPoEoA sessions with dynamic bandwidth selection (DBS) enabled on a single PVC, the VC inherits the QoS, peak cell rate (PCR), and sustained cell rate (SCR) values from the session with the highest parameter; however, the VC incorrectly inherits the watermarks and channel weight from the last session authenticated on that VC.

There is no known workaround.

CSCse57404

A router running IOS 12.3(7)X17 may experience memory fragmentation such that the largest block of memory shrinks gradually over time when running TCP header compression. The fragmentation can be seen over a period of time by looking at multiple captures of the **show memory statistics** command.

Workaround: Reload the router before the fragmentation becomes too severe.

CSCse58765

A Cisco 7200 router with NPE-G1 may fail by Red Zone memory corruption at the I/O pool. The Cisco 7200 router is running Cisco IOS 12.3(7)XI6 and configured to handle VPDN services from PPPoE users.

There are no known workarounds.

CSCse59991

Flow bit setup induced a failure when configuring 1-Port Channelized OC-12 line card.

There are no known workarounds.

CSCse60811

PRE2 failure is related to a QoS config policy-map change.

There are no known workarounds.

CSCse61797

A class VC may stop passing traffic and generates the following error:

```
%ATM-3-FAILCREATEVC: ATM failed to create VC(VCD=110, VPI=61, VCI=43) on Interface
ATM1/0/0, (Cause of the failure: VC Creation has failed due to a platform-specific limit)
```

Workaround: Remove the class VC.

CSCse62405

PRE2 fails during LCP session cleanup.

There are no known workarounds.

CSCse65406

A FPGA buffer leak may cause serial interfaces to not forward traffic. This occurs on the Cisco 10008 router with a 4-Port Channelized OC-3 or 1-Port Channelized OC-12 line card.

Workaround: There is no known workaround but resetting the line card may resolve the issue.

CSCse66110

The router fails while processing security turbo-ACLs. This occurs when the router is running Cisco IOS Release 12.3(7)XI7.

There is no known workaround.

CSCse82618

The router reports incorrect values for the half-height Gigabit Ethernet counters (ifHCInOctets).

There is no known workaround.

CSCse91763

Under certain conditions, the router does not forward traffic out the ATM line card. This is believed to occur after deleting and then recreating VCs. However, the exact conditions are unknown.

Workaround: Issue the **shutdown** or **no shutdown** command on the affected subinterface.

CSCse94557

RIP is used to advertise a route from the access router to the Cisco 10000 series router. When the route is changed so that it is bound to another interface, the **show ssg binding** command does not display information about the changed condition. This occurred on a Cisco 10000 series router running Cisco IOS software based on Cisco IOS Release 12.3(7)XI7. The following commands display the correct information:

- **show ip route IP**
- **show pxf cpu cef vrf name network network**
- **show pxf cpu vcci**

There is no known workaround, but to ignore the output of the **show ssg binding** command.

CSCsf01333

The Cisco 10008 router might restart due to a bus error. This occurs when the router is running Cisco IOS Release 12.3(7)XI7b.

There is no known workaround.

CSCsf04178

When you add a prefix-list entry to a prefix-list in a redistribution route map, the entry does not take effect. This occurs when using a redistribution route map to filter static routes that are specified in the prefix-list.

Workaround: After adding the configuration change, enter the **clear ip route prefix** command.

CSCsf11736

The PRE2 fails at atm_nvgen_static_map. This occurs with approximately 8000 sessions established, and with call churn and scripts running and performing the following operations:

- Overwriting VC classes
- Removing and adding service policies
- Issuing various **show** commands

There is no known workaround.

CSCsf19152

ICMP replies are not identified properly by PE-LNS.

There is no known workaround.

CSCsf19340

When the router resets the 4-port OC-3/STM-1 ATM line card, the PXF fails and the following messages appear in the log file. This occurs on a Cisco 10008 router running Cisco IOS Release 12.3(7)XI8.

```
%C10K_ALARM-6-INFO: ASSERT CRITICAL slot 1 Card Stopped Responding OIR Alarm - subslot 0
%LINK-3-UPDOWN: Interface ATM1/0/3, changed state to down
%C10KEVENTMGR-4-PXF_CRASHINFO: Writing PXF debug information to
bootflash:pxf_crashinfo_20060824-080444.
%C10KEVENTMGR-1-MAJOR_FAULT: PXF DMA Error - Small Packet Handle Creating a Large
Descriptor, Restarting PXF
```

There is no known workaround.

CSCsg03962

The router is unable to parse ACLs if the ACLs are downloaded per user, the ACL contains a syntax error, or the router reaches system limits.

Workaround: Configure fewer ACLs downloaded per user or repair the syntax.

CSCsg07532

PXF fails with a PXF DMA TBB Length Error.

There is no known workaround.

CSCsg19563

The **show caller** command is inaccurately showing sessions as exceeding the idle time even though the user has already dropped.

There is no known workaround.

CSCsg37434

Unable to add virtual access interface (VAI) to the no phy_subif list.

There is no known workaround.

CSCsg37674

A router receives unknown packets with an encapsulation type of 0 from a PPPoE session running on an ATM VC. The router drops the packets with no impact on services. This occurs when PPP auto-cleanup is configured on a router that is running Cisco IOS Release 12.3(7)XI.

There is no known workaround.

CSCsg40859

If a router is using high CPU use for a virtual template BGR process and the CNS agent is enabled, subsequent polling of the router causes a failure to occur.

Workaround: Reconfigure the router to decrease the high CPU use.

CSCsg41396

The Cisco 10000 series router sends duplicate PPP IPCP CONFREQ packets in the outbound direction.

There is no known workaround.

CSCsg53427

A traceback message is observed at 10k_atm_vc_state_change when you apply or remove a VC class from an interface with active VCs and you issue a **shutdown** or **no shutdown** command from a Telnet (vty) session

There is no known workaround.

CSCsg53585

Users are unable to log into services. This occurs sporadically when the router is used for SSG RBE aggregation. Users are able to reach the web portal and log in properly, but they are unable to access any of the services.

Workaround: Remove the **pvc range** command from the service in question and then add it back.

CSCsg61035

A policy map with three levels does not operate correctly. If you add a grandchild policy map to a child policy map when the top parent policy map is already attached at the interfaces, QoS queuing and policing break.

Workaround: Detach the parent policy map from the interface and then reattach it. This action should return QoS queuing and policing functionality to normal.

CSCsg65975

Attempts to free the AAA database of accounting stop messages causes a failure to occur.

There is no known workaround.

CSCsg72898

Alignment errors and traceback messages occur after applying some per-user attributes.

There is no known workaround.

Resolved Caveats—Cisco IOS Release 12.3(7)XI10a

This section describes caveats that were fixed in Cisco IOS Release 12.3(7)XI10a.

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

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

CSCdy14140

Cisco IOS software sometimes reloaded with a bus error at tcp_outputpending after two users issued the **show running-config** command and the **format slot0** command in parallel over VTY. This has been fixed.

CSCea87385

CISCO-RF-MIB traps were enabled automatically after a chassis reload. This has been fixed.

CSCeb05456

The router sometimes reset its route processor (RP) when two simultaneous **write memory** commands from two different VTY connections were executed. A message similar to the following sometimes appeared in the crashinfo file. This occurred intermittently and was related to the way the NVRAM was accessed. Although it was observed on a Catalyst 6000 series Supervisor Engine 720 running Cisco IOS Release 12.2(18)SXD, it was platform and release independent. This has been fixed.

```
validblock_diagnose, code = 10

current memory block, bp = 0x48FCC7D8,
memory pool type is Processor
data check, ptr = 0x48FCC808

next memory block, bp = 0x491AC060,
memory pool type is Processor
data check, ptr = 0x491AC090

previous memory block, bp = 0x48FCBBE8,
memory pool type is Processor
data check, ptr = 0x48FCBC18
```

CSCeb70195

The line loopback was not using the line clock. This has been fixed.

CSCec86624

Traffic convergence after the removal of APS on the 1-port channelized OC-12 line card was greater than 2 seconds. This has been fixed

CSCed64631

A PPP session should not start for service-type=login. A RADIUS response may ignore the framed-protocol attribute when it is an unsupported protocol. An attribute list might be created from this RADIUS response without the framed-protocol attribute. In this situation, PPP may not find the framed-protocol attribute and may continue the session. This has been fixed.

CSCed81202

The HWTAG:Invalid s/w taginfo error message was occasionally displayed after an interface transition. This has been fixed.

CSCee05882

When an MLPPP bundle has an output policy attached to an interface and the service policy contains WRED parameters, the policy might contain the wrong queue size after the router reloads. This has been fixed.

CSCef47280

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

On a Cisco 10000 series router, if you configured the AU-4 T1 interface on a 4-port channelized OC-3 line card that was connected to a 3rd party test analyzer device on the far end with the same configuration, the T1 interface did not come up. This has been fixed.

CSCef77013

Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also result in a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not result in a crash of the device itself, but may result in a crash of the IPv6 subsystem.

Cisco has made free software available to address this vulnerability for affected customers. 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-20070808-IOS-IPv6-leak.shtml>.

CSCef94552

In an MPLS VPN scenario, a PE configured with ISDN backup for MPLS might be unable to forward packets over the backup link. The LDP session comes up and labels are correctly exchanged, but even though the label information base (LIB) contains the labels, they are not populated into the Label Forwarding Information Base (LFIB); entries appear there as untagged. Also, the TAG adjacency for the Dialer interface remains incomplete. This has been fixed.

CSCeg48971

The command to display cached PPPoE configuration information was present in Cisco IOS 12.3T images, but not in Cisco IOS Release 12.3(7)X13. The affected command was **show pppoe derived**. This has been fixed.

CSCeg49366

When output policing was occurring on the OC-48 POS line card and you entered the **show policy-map** command, the counters displayed incorrect information. This has been fixed.

CSCeg52893

VTY/TTY sessions sometimes stopped responding after unsuccessfully attempting to authenticate to an external AAA server. External authentication failed before the maximum number of AAA attempts were reached locally. The **show line x** command displayed the following message for a line that was still considered active. This has been fixed.

```
Modem state: Ready, Carrier Dropped
```

CSCeg62206

When high CPU use occurred on the core router, the router locked up and could not be accessed using Telnet or console. The TPLUS process was holding nearly 50-60 percent of the CPU at this time. This has been fixed.

CSCeg83467

The router crashed whenever encapsulation changed from AAL5SNAP to AAL0 on a private virtual circuit (PVC). This has been fixed.

CSCeg90131

When a service policy was applied to a channelized T3 virtual routing and forwarding (VRF) interface, changes to the percentage of bandwidth to allocate to a traffic class that is defined in the service policy was causing the policy to be removed from the interface. This has been fixed.

CSCeh30518

The queue-limit under queue is not taken when a policy-map is already attached with a child policy-map. This has been fixed.

CSCeh39267

IPCP did not allocate a DHCP IP address when PPPoE sessions were brought up. This occurred when PPP used DHCP to allocate an address to the remote subscriber. This issue occurred in the following two places:

- Subnet allocation client side—Accepted the 10 minute or less lease time without complaint
- Subnet allocation server side—Allowed the 10 minute or less lease time to be configured on the subnet allocation pool

The lease time must be configured greater than 10 minutes as a safety check for misconfiguration. This has been fixed.

CSCeh58848

Police counters went to the maximum value when the police configuration was changed. This has been fixed.

CSCei16493

When a single router-APS (SR-APS) configuration was removed and re-applied, continuous traceback messages were generated on the standby PRE2. This has been fixed.

CSCei49897

PXF queues of variable bit rate (VBR) VCs were being removed. This has been fixed.

CSCej76195

Cisco 10000 series routers experienced spurious accesses while running PPPoEoA, DBS (Dynamic Subscriber Bandwidth Selection) and moderate downstream traffic. This has been fixed.

CSCek00596

When running Multilink PPP (MLP) traffic, the PXF failed with some type of DMA command error such as "PXF DMA OQC at End of Descriptor With Non-Zero Continuation Bit." This occurred when numerous MLP bundles were configured and there was also a high amount of traffic creating a shortage of packet buffers. This has been fixed.

CSCek37564

On the Cisco 10000 series router, performance drops to approximately 95 percent when using packet sizes of 110 and 238 bytes. This has been fixed.

CSCek39034

The PPPoE VSF circuit-id tag debug was missing from the client. This has been fixed.

CSCek40657

The PPP termination and aggregation (PTA) failed while downloading the configuration. This has been fixed.

CSCek44183

A memory leak was occurring at 10k_atm_tearardownvc_bulk when PPPoA sessions were established on a VC range. This has been fixed.

CSCek47264

A traceback message occurs when simultaneously reconfiguring the router in console and Telnet mode. For example, issuing the **class-int pppoa** command at the console and simultaneously issuing the **shutdown** or **no shutdown** command in a Telnet session causes a traceback message to appear. This has been fixed.

CSCek48136

The router sometimes failed when QoS policy changes occurred for a large number of VCs. This was observed on the router when an automated script was used to make the QoS changes. This has been fixed.

CSCek53988

The following error message appeared on the router console when automatic protection switching (APS) was enabled. This occurred on the Cisco 10000 series router with either a 1-port channelized OC-12 line card or a 4-port channelized OC-3 line card. The error message appeared when issuing the command to enable APS after the configuration was loaded. The error happened if the router had a very large configuration and interfaces were configured on the line card that became the protection card. This has been fixed.

```
%SYS-2-INTSCHED: suspend at level 3 while config CH_STM1-APS
```

CSCek54768

E1 interfaces sometimes stopped responding when a line card was reset or removed, even if the line card had APS enabled and an APS switchover was triggered. The interfaces did come back up within a few seconds. This occurred on a Cisco 10000 series router with a pair of 4-port channelized OC-3 line cards that were configured for single-router APS (SR-APS). The line cards were configured with E1 interfaces under either SONET or SDH. The symptom occurred only when a line card was reset or removed, not when an APS switchover was triggered by a fiber cable that was removed. A change in the E1 clock source that sometimes occurred when the line card was reset or removed caused the router to receive alarms. The symptom occurred more often when the line card had a large configuration and when the E1 interfaces were set to “clock source line.” This has been fixed.

CSCek55136

The Cisco 10008 router was sometimes restarting due to a bus error if the router was running Cisco IOS Release 12.3(7)XI7b. This has been fixed.

CSCek56775

An unwarranted message was reported when a user-defined class with priority was added to a policy-map with only the class-default class defined. The router did not accept the priority action in the class. You should not configure a priority class in a child policy if the parent policy has only the default class with only a shape action defined. This has been fixed.

CSCek63422

QoS-related traceback messages were seen on either the PPP termination and aggregation (PTA) router or the L2TP access concentrator (LAC) when scaling to 48,000 or 62,000 sessions. These sessions were over ATM, Ethernet, Ethernet over ATM, Ethernet over ATM over VLAN with different combinations of encapsulations. This has been fixed.

CSCek63673

On a virtual access interface (VAI) for PPP over ATM (PPPoA) sessions, the Cisco IOS software did not configure the ingress netflow. When you issued the **show ip cache flow** command, no flows appeared. This has been fixed.

CSCeh97080

When Multiprotocol Label Switching (MPLS) is enabled on a router, one or more LDP sessions might be disrupted during periods of extremely high CPU use. This has been fixed.

CSCin61143

In versions of Cisco IOS Release 12.3(02.03)B and Release 12.3(04)T01 012.003, the IETF Calling-Station-ID attribute 31 sent clid/dnis as a single string. The slash (/) in the string caused the dnis part of the string to become corrupted. The dnis part was included in the Called-Station-ID attribute 30. This affected accounting and authorization records. This has been fixed.

CSCin87312

Addresses given to the client were not from the assigned Ascend-IP-Pool. The IP address is assigned from a pool (Ascend-IP-Pool) of addresses that are kept by the NAS. When RADIUS sends a Framed-IP-address of value 255.255.255.255 and a valid Ascend-IP-Pool, then the NAS should allow the peer to select an IP address from the default IP pool. This has been fixed.

CSCin98817

PDSN running YF2 based engineering special was reloaded due to a bus error. The reload occurred while deleting the PPP conditional debug. This is a rare event as the bus error occurs only when the deletion of the PPP conditional debug happens simultaneously with the connection deletion. This has been fixed.

CSCin95836

The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

NHRP is not enabled by default for Cisco IOS.

This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml>.

CSCir00074

The router failed when `casnDisconnect` was set to “true” for a PPPoE session. This has been fixed.

CSCir01290

When an ATM interface was in the shutdown state and a hold queue length was configured with a non-default length, rebooting the router caused the interface to stay in the Down state. This problem occurred only when the router was running Cisco IOS 12.3(7)XI software. This has been fixed.

CSCsa53117

Potential MLS cef freeze if interface status changed. MLS cef freeze was occurring when an interface was shut down or VRF routes were changed and no other interfaces could be provisioned. This also caused ping/connectivity problems. This has been fixed.

CSCsa58340

Police command triggered software reload. The reload occurred if the policy map being edited already contained the maximum number of classes that the router supports and an attempt to add one more class is made. This has been fixed.

CSCsa84298

Request was made to report the total subscribed rate for a VP (sum of SCRs). This has been fixed.

CSCsb06200

For preauthorization using Service-type Outbound, calls could fail with the error “Unsupported Service-Type: 5. No supported types found.” This has been fixed.

CSCsb07279

The Cisco IOS software did not see a new IPv4 prefix list added to the route map that ISIS redistributes. This has been fixed.

CSCsb57122

When you attached a non-nested policy map to an interface, the following message sometimes appeared, even if you configured a valid shape rate. This occurred on a PRE2 running either Cisco IOS Release 12.2(27)SBB or Release 12.3(7)XI. This has been fixed.

```
Shape rate too low for GigabitEthernetXXX
```

CSCsb97607

On the Cisco 10000 series router, it was observed that when the BIP-2 counters were not cleared for a long time, the counters showed an increasing number of errors each 15-minute period. It appeared that the BIP-2 value of the “Current Interval” was added to the “Start Values” of the 15-minute periods on the channelized STM-1 line card. This has been fixed.

CSCsc31958

Spurious memory accesses after the **show policy-map interface** command is issued on an ATM PVC. This has been fixed.

CSCsc40078

When a class in a service policy is configured with 1 percent of the remaining bandwidth, the **show policy-map interface** command output displays 0 as the weight value for this class. This is just a display issue. No functionality is impacted by this problem. This has been fixed.

CSCsc42260

BW is not released from the class-default after FR pvc is deleted/re-defined. This has been fixed.

CSCsc56407

Non-priority traffic goes through the priority queue. This has been fixed.

CSCsc84506

Cannot add interface descriptions on Virtual-Access sub-interfaces. This has been fixed.

CSCsc91155

A Cisco IOS Release 12.3(7)XI7 failure generated the following error. This has been fixed.

```
%C10K_QUEUE_CFG_GENERAL-2-EREVENT
```

CSCsd81407

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

CSCsd03001

When the following alarm was set, it appeared that the way to clear it was to reset the standby. In some cases however, resetting the standby did not clear the alarm because it became set again. The alarm condition appeared using the **show facility-alarm status** command and the Major Alarm LED on the faceplate was lit. This has been fixed.

Source: RP A Severity: MAJOR ACO: NORMAL Description: Secondary not synchronized

CSCsd59028

Error message appeared when Frame Relay subinterfaces were created. This has been fixed.

CSCsd61220

An oversubscribed warning occurred when a hierarchical policy was removed from the main interface or when the hierarchical policy was applied twice to the main interface of any line cards. This has been fixed.

CSCsd61680

Configuring a static ARP entry that points to a node on a QinQ subnet caused a traceback to appear. This has been fixed.

CSCsd69365

Executing the **dir all-f** command caused the CPU use to become high. This has been fixed.

CSCsd72336

When using Lawful Intercept, CPU use can reach 100 percent. This occurs when the tap is set on an IP address for which there is no entry in the global routing table or when the tap is set on an IP address for which the closest match is a supernet in the global routing table. This has been fixed.

CSCsd77078

Ping over serial interfaces failed during a U2 run because the output VCCI was not being set correctly. This has been fixed.

CSCsd82487

PXF routing failed for GigE main interface traffic because the PXF CEF entry for the main interface was improperly programmed to VCCI 0 for destination entries that point to next-hop. This has been fixed.

CSCsd86963

Removing a GigabitEthernet subinterface with SSG configured was causing a forced failure. This has been fixed.

CSCsd87213

The **getmany** command did not return the available devices name for the CISCO-FLASH-MIB on the Cisco 10000 series router. This has been fixed.

CSCsd87867

Maximum burst size was not configurable on an ATM VBR-nrt PVC. This has been fixed.

CSCsd94129

After PPP was configured and ISIS was subsequently enabled, the router failed to negotiate OSICP for ISIS adjacencies. Encapsulation failures were seen and PPP rejected the OSICP continuously. This has been fixed.

CSCse27599

Applying policing with IP type of service (ToS) classification caused the router to drop packets, but the output from the **show policy interface tunnel #** command did not indicate that the packets were classified or dropped. However, the **show pxf cpu stat qos** command did display information indicating that the packets were classified. This occurred when a router configuration consisted of a PRE2 with Ethernet over multicast (EoM), any transport over multicast (AToM), or Layer 3 VPNs configured, and GRE tunnels were configured between the source and receiving router on various interfaces. This has been fixed.

CSCse34173

Some of the serial interfaces became stuck in an up or down state, and traceback messages and FIFO drain errors occurred. This occurred when the router performed a PRE failover, reset a line card, or reloaded the PXF, or when multilinks flapped because a large number of multilinks were configured with traffic that consists of smaller IP packets. Issuing a **shutdown** or **no shutdown** command on the multilinks or member links did not recover the interfaces from the up or down state. This has been fixed.

CSCse41999

When using PPPoE, packets sent to the route processor (RP) were counted two times in the interface statistics. This occurred when the PXF received the packet, incremented the counters, and sent the packet to the RP for processing. The RP then incremented the counters, which resulted in the double-count. This has been fixed.

CSCse42235

The Packet of Disconnect (POD) conversion to internal ID was not working with account prepend information. This has been fixed.

CSCse49188

Reconfiguring an ATM PVP was causing inconsistencies between the primary and secondary PRE. This caused the secondary PRE to reload and resynchronize with the primary PRE. This has been fixed.

CSCse52763

Changing the parent shaper value on a hierarchical policy (by using the **no shape rate** or **shape rate** commands) attached to a Frame Relay interface, or Fast Ethernet or Gigabit Ethernet interface results in the removal of all queues other than the class-default and pak_priority queues on the interface. All traffic belonging to the other queues is dropped. This has been fixed.

CSCse57324

The router did not report SONET Link Up and Link Down event messages for the protection port of an APS pair. This occurred on the Cisco 10000 series router with a single-router APS (SR-APS) configuration on the 4-port channelized OC-3 line card. When the fiber was removed from the protection port to simulate a failure on the protection line, the router did not send a message to the console log. This might have also affected other line cards on the router that support SR-APS. This has been fixed.

CSCse62507

An nf_export_pkt_handle assertion error occurred in simulation. This has been fixed.

CSCse68138

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

CSCse68580

The watchdog timer caused failures on the STATS DMA daemon. This has been fixed.

CSCse70998

The PRE-2 I/O FPGA Illegal Access interrupt handler was not clearing the I/O FPGA Illegal Access interrupt, causing the software to loop indefinitely. This has been fixed.

CSCse76134

The router images in the 12.3(7)XI and 12.2S software branches did not include ppp_fast.o. This has been fixed.

CSCse77657

Unable to configure policer on c-def if 64-class nest pmap applied to PPP session. This has been fixed.

CSCse81287

The resolution for CSCse66783 could potentially cause a packet ordering problem. This has been fixed.

CSCse83989

Resetting or inserting a line card while traffic is flowing caused the line card to reset continuously. This has been fixed.

CSCse84099

On the Cisco 10000 series router, the T3 or VT controllers sometimes did not come up when you configured the C2 overhead byte under SONET T3 or VT controllers on a 1-port channelized OC-12/STM-4 line card or a 4-port channelized STM-1/OC-3 line card. This has been fixed.

CSCse84350

ATM VCs go down in combination with OAM and DBS. This has been fixed.

CSCse85200

Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behavior by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router. Since CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment. This has been fixed.

CSCse89105

When RADIUS packets are sent to a Cisco router configured for Service Selection Gateway (SSG), SSG allocated extra memory and reduced the packet size, which created issues for other components. The router showed RADIUS packets being dropped while the RADIUS packets were sent. This occurred when a RADIUS packet with a length of more than 1024 bytes was sent. This has been fixed.

CSCsf07424

The line card reloads users who are disconnecting and the system was malfunctioning because the PXF sent a heavy rate of traffic to the route processor (RP). Buffer depletion created allocation failures, causing the system to fail. This has been fixed.

CSCsf07847

CDP may fail to discover neighbor information. This has been fixed.

CSCsf17577

When the Cisco 10008 router switched traffic into an L2TP tunnel, the router was not always accounting for the switched traffic. For example, when downloading a file (with a known file size) through an L2TP tunnel that terminated on a Cisco10000 L2TP network server (LNS), the interface counters and AAA accounting sometimes displayed less traffic than what was actually downloaded. The following message sometimes appeared in the router log files:

```
%GENERAL-4-WRNEVENT: Incomplete Stats Collection
```

This only affected L2TP traffic. It did not affect traffic that was not sent through an L2TP tunnel or through a tunnel using any other protocol. This has been fixed.

CSCsf19133

When SNMP polled the cbQosPolicyMapCfgTable object of the CISCO-CLASS-BASED-QOS-MIB, it was not retrieving the child policy maps that were applied to a class in a parent policy map. This occurred when the Cisco 10008 router was running Cisco IOS Release 12.3(7)xi7e. This has been fixed.

CSCsg07084

The PXF punted incoming ARP requests to the route processor (RP) without first verifying that the requests were valid. This has been fixed.

CSCsg15342

Cisco 10000, uBR10012 and uBR7200 series devices use a User Datagram Protocol (UDP) based Inter-Process Communication (IPC) channel that is externally reachable. An attacker could exploit this vulnerability to cause a denial of service (DoS) condition on affected devices. No other platforms are affected.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-ipc.shtml>.

CSCsg28139

The platform MPLS code was using old definitions to get VLAN IDs. It did not match either the header file or the source file. This has been fixed.

CSCsg30882

All ATM PVCs were becoming inactive (INAC) for an interface. This has been fixed.

CSCsg31453

An ATM configuration change could cause the SAR to reload. VCs could flap once (get torn down and immediately be recreated) on all ports when an ATM CLI was entered if there was a setting for the MTU other than the default. This has been fixed.

CSCsg37876

The following Badshare messages occurred during the router boot sequence. This has been fixed.

```
*Oct 12 03:08:20: %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=201F90EC, count=0
-Traceback= 60408E70 60092E04 60092E84 60414D90 60C65F24 60C429F0 60877E5C 60852608
6084AF0C 6085A570 6085887C 60849F80 6084A348 60487A74 6084A36C 604862B4
Oct 12 16:48:52: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x60D763E0 reading 0x8
Oct 12 16:48:52: %ALIGN-3-TRACE: -Traceback= 60D763E0 60D69C8C 604D8340 604F5A2C 60087EF0
60087C00 6017BE30 60C50B78
```

CSCsg40737

After issuing the **clear pppoe all** command, the router failed. This occurred when PPP events triggered high CPU use. This has been fixed.

CSCsg42502

Potential red zone overrun in the 10k_buffer_monitor. Although the buffer dump function of the 2RP policer was set up safely, under certain conditions if the limit of the buffer was not reached the next buffer could be so big that it overwrote the assigned space. This has been fixed.

CSCsg45130

When online insertion and removal (OIR) of a line card occurred and SNMP was enabled, occasional SONETMIB-1-DELETE: error messages appeared. This has been fixed.

CSCsg76652

A freed packet was sometimes passed on for additional processing. This has been fixed.

CSCsg81770

A subinterface with an ifIndex=62 did not show up in ifMIB output. When the router was configured such that the ifIndex value of 62 got assigned to a subinterface (non-HWIDB), the interface sometimes did not show up in the ifMIB. This has been fixed.

CSCsg83816

SNMP did not report physical interfaces after a line card was removed and reinserted on the same slot in the router. The **show snmp mib ifmib ifindex** command still reported ifindexes, but the **debug snmp packet** command indicated that the router was no longer sending physical interface ifindexes. The SNMP Management server did not receive ifindexes either. Only physical interfaces were not reported; ifindexes for subinterfaces or any other line card elements were not affected. This has been fixed.

CSCsg84381

When SSG was reloaded, the **ssg tcp-redirect** command only worked if you removed or re-added the **ssg direction downlink** command on a specific ATM subinterface. This occurred when a user opened the browser and then SSG redirection was performed. SSG redirected the HTTP request to the SESM server, but SSG did not change the SESM response from the IP address of SESM to the initial user destination IP address. As a result, the SESM server replied to the user with its own IP address and the user reset the connections. This has been fixed.

CSCsg84522

The router failed because of Inverse ARP (INARP) managed timer issues. This occurred when the INARP timer was configured or unconfigured. This has been fixed.

CSCsg86572

For a multi-router APS (MR-APS) configuration, after issuing the **hw-module slot 1 shut** command on the Working router and issuing the **show aps** command, the slot still showed active. The interface of the down line card showed Link up and Protocol down. The Protect router was then active and passing traffic. When the **no hw-module slot 1 shut** command was executed, the Protect router became inactive and the Working router became active. This occurred only when issuing the **hw-module slot slot-number shut** command and the **hw-module slot slot-number reset** command. It did not occur when the SONET controller was shut down. This has been fixed.

CSCsh06896

The following error message was observed. This has been fixed.

```
%C10K_QUEUE_CFG_GENERAL-2-EREVENT: Error @../toaster/c10k_rp/c10k_tt_q
```

CSCsh16497

When you started the router with a clean startup configuration and then you configured the **bba-group pppoe name** command, the router sent the following message to the console log every 10 seconds after the virtual access interface (VAI) came up. This has been fixed.

```
"%GENERAL-4-WRNEVENT: Incomplete stats collection"
```

CSCsh30298

The following message was observed in the log on a Cisco 10000 series router with a PRE2 using Cisco IOS Release 12.3(7)XI. This has been fixed.

```
%SYS-3-MGDTIMER: Uninitialized timer; Process= DHCPD Receive
```

CSCsh40178

On a Cisco 10000 series router with a PRE3, PPPoX client interfaces sometimes did not show packet counters, which resulted in difficulties troubleshooting problems or verifying traffic. This occurred with configurations of thousands of PPPoX per-session QoS sessions with traffic running and was not limited to the Cisco 10000 series router. This has been fixed.

CSCsh51445

Lawful Intercept did not reference the correct interface. If two routes to a given network exist with different subnets, Lawful Intercept applied the tap on the more summarized route instead of the less summarized one. This has been fixed.

CSCsh52590

When you entered **show vlan** commands with large amounts of data to be processed, the router sometimes displayed the following error message in the virtual EXEC process. This has been fixed.

%SYS-3-CPUHOG:

CSCsi01470

A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>.

CSCsi01927

Encapsulation diverts sometimes increased rapidly and sent CPU use very high. To fix this, an enhancement was added to police or drop encap diverts. This new functionality added a new 2 RP queue to tail drop rate-limited encap diverts. The **ip pxf encap-divert drop** command was added to allow the encap diverts to be completely dropped, instead of being punted to the RP.

CSCsi13736

The PXF engine classifies packets based on the IP version of the packet. Previously, when an IP header had a version identifier that was not equal to 4, the PXF sent the packet to the RP for processing. However, Cisco IOS Release 12.3(7)XI software does not support IPv6 RP processing.

Cisco IOS Release 12.3(7)XI10a software changes the way in which non-IPv4 packets are managed. Instead of forwarding non-IPv4 packets, including IPv6 packets to the RP, the PXF drops all packets with IP version identifiers other than 4. This means the PXF now blocks IPv6 operations that were previously processed on the RP.

Cisco IOS Release 12.2SB includes the functionality to officially support IPv6 RP processing in the PXF. To do IPv6 operations on the RP, upgrade to Cisco IOS Release 12.2SB. For more information, see the “Upgrade Option 4: ESR-PRE2 Upgrade with RPR Switchover” section in the *Upgrading to Cisco IOS Release 12.2(28)SB on a Cisco 10000 Series Router* guide at:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_upgrade_guides09186a008059adee.html#wp37787

CSCsi15995

All interfaces stop transmitting traffic after PRE failover.

CSCsi18523

PPPoEoE packets are not forwarded over native VLAN.

CSCsi46897

PRE crashes after snmpwalk on MIB cbQosSetStatsTable.

CSCsi60004

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254

- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

CSCsi69009

High CPU in the IPCP due to continuous renegotiating by clients.

Obtaining Documentation

For information on obtaining documentation and support, providing documentation feedback, security guidelines, and recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*. After the list of new and revised Cisco technical documentation, click the links beginning with **Obtaining Documentation** in the table of contents at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)

