



Release Notes for the Cisco 10000 Series Router for Cisco IOS Release 12.3(7)XI8

First Published: June 30, 2006

Revised: January 24, 2007

OL-10914-01

These release notes provide information about Cisco IOS Release 12.3(7)XI8, which provides broadband aggregation, leased-line, and MPLS features for the Cisco 10000 series router.

Cisco IOS Release 12.3(7)XI8 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)XI8, see the “[Caveats for Cisco IOS Release 12.3\(7\)XI8](#)” section on page 13 and *Caveats for Cisco IOS Release 12.3T*. The caveats document is updated for every maintenance release and is located on [Cisco.com](#).

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

Cisco IOS Release 12.3(7)XI8 is based on the following releases:

- Cisco IOS Release 12.2(16)BX
- Cisco IOS Release 12.3T
- Cisco IOS Release 12.3(7)XI8

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

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

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

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



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

© 2006 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\(7\)XI8, page 3](#)
- [Limitations and Restrictions, page 3](#)
- [Important Notes, page 10](#)
- [Caveats for Cisco IOS Release 12.3\(7\)XI8, page 13](#)
- [Obtaining Documentation, page 82](#)
- [Documentation Feedback, page 83](#)
- [Cisco Product Security Overview, page 83](#)
- [Obtaining Technical Assistance, page 84](#)
- [Obtaining Additional Publications and Information, page 85](#)

System Requirements

Cisco IOS Release 12.3(7)XI8 requires that you have the performance routing engine (PRE), Part Number ESR-PRE2 installed in the Cisco 10000 series router chassis. To verify which PRE is installed in the router, use the **show version** command.

Route Processor Redundancy Mode

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

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

Table 1 lists the RPR modes used when upgrading or downgrading Cisco IOS software. For example, when upgrading to Cisco IOS Release 12.3(7)XI8 from Release 12.2(16)BX, the router uses RPR mode instead of RPR+ mode. When downgrading to Cisco IOS Release 12.2(16)BX from Cisco IOS Release 12.3(7)XI8, the router uses RPR mode.

Table 1 RPR Modes for Cisco IOS Software Releases

Releases	12.2(16)BX	Cisco IOS Release 12.3(7)XI8
12.2(16)BX	RPR+	RPR
12.3(7)XI7	RPR	RPR+
12.3(7)XI8	RPR	RPR+

Before You Upgrade the Cisco IOS Software

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

Upgrading to a New Software Release

For specific information about upgrading your Cisco 10000 series router to a new software release, refer to the *Cisco 10000 Series Router Performance Routing Engine Installation*.

<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)XI8

Cisco IOS Release 12.3(7)XI8 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 the following URL:

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

For more information about this new feature, see the document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xi7/gt_qinq.htm

Limitations and Restrictions

This section describes limitations and restrictions for the following areas. Be sure to review the following limitations and restrictions before using the features in Cisco IOS Release 12.3(7)XI8:

- [Binding a Service to Broadcast Interface, page 4](#)
- [Complete ID, page 4](#)
- [Controlling the Rate of Logging Messages, page 4](#)
- [DBS Extensions, page 5](#)
- [DNS Fault Tolerance, page 5](#)
- [DNS Redirection, page 5](#)
- [Frame Relay, page 5](#)
- [Full VAs, page 5](#)
- [Half-Duplex Virtual Routing and Forwarding over Route Bridge Encapsulation, page 5](#)
- [IEEE 802.1Q-in-Q VLAN Tag Termination, page 5](#)
- [L2TP Dialout, page 6](#)
- [PDSN Interworking, page 6](#)

- [Per Session Queuing and Shaping for PPPoE VLAN Using RADIUS](#), page 6
- [PRE Network Management Ethernet Port](#), page 7
- [PTA MD](#), page 7
- [Radius Proxy Enhancements for CHAP](#), page 7
- [Range Command for Bind Statements](#), page 7
- [Redundant Uplinks to the Same Service](#), page 8
- [Scalability](#), page 8
- [Service level ACLs](#), page 8
- [SSG Auto Logoff](#), page 8
- [SSG EAP Transparency](#), page 8
- [SSG GRE](#), page 8
- [SSG IOS NAT](#), page 9
- [SSG L2TP](#), page 9
- [SSG Prepaid](#), page 9
- [Support for Classifying Hosts Based on IP Address](#), page 9
- [Suppression of Unused Accounting Records](#), page 9
- [Testing Performance of High-Speed Interfaces](#), page 9
- [Unique Session ID](#), page 9
- [VRF-Aware VPDN Tunnels](#), page 10

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 ESR 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, make sure the issue is not the same as CSCsc83107

Half-Duplex Virtual Routing and Forwarding over Route Bridge Encapsulation

HDVRF over 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.

L2TP Dialout

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 command line interface (MQC) 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 for telnet, SNMP, etc. The interface used for system management cannot terminate PPPoE or L2TP sessions.

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 will then bind 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 will always traverse the service they have subscribed to first, regardless of the ultimate destination or original source.

A host can not 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

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 create on demand PVCs (individual and within a range) and PPP sessions, RP CPU utilization can be extremely high when bringing up and tearing down sessions and PVCs. This is only a concern when the configuration contains approximately 30,000 PPP sessions, and additional services 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 utilization.

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. The connection will remain active, but the ACLs will 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 10](#)
- [Enhancing Scalability of Per-User Configurations, page 11](#)
- [Inserting a New Line Card, page 12](#)
- [Provisioning for Scaling, page 12](#)

Configuring the `aaa new-model` Command

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



Note

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

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

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

Enhancing Scalability of Per-User Configurations

To enhance scalability of per-user configurations without changing the router configuration, use the **ip:vrf-id** 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** is used to map sessions to VRFs. Any profile that uses the **ip:vrf-id** VSA must also use the **ip:ip-unnumbered** VSA to install IP configurations on the virtual access interface that is to be created. PPP that is used on a virtual access interface to be created requires the **ip:ip-unnumbered** VSA. An Internet Protocol Control Protocol (IPCP) session is not established if IP is not configured on the interface. You must configure either the **ip address** command or the **ip unnumbered** command on the interface so that these configurations are present on the virtual access interface that is to be created. However, specifying the **ip address** and **ip unnumbered** commands on a virtual template interface is not required because any pre-existing IP configurations are removed when the **ip:ip-vrf** VSA is installed on the virtual access interface. Therefore, any profile that uses the **ip:vrf-id** VSA must also use the **ip:ip-unnumbered** VSA to install IP configurations on the virtual access interface that is to be created.

These per-user VSAs can be applied to virtual access subinterfaces; therefore, the per-user authorization process does not require the creation of full virtual access interfaces, which improves scalability.

Setting VRF and IP Unnumbered Interface Configurations in User Profiles

Although the Cisco 10000 series router continues to support the **lcp:interface-config** VSA, the **ip:vrf-id** and **ip:ip-unnumbered** VSAs provide another way to set the VRF and IP unnumbered interface configurations in user profiles. The **ip:vrf-id** and **ip:ip-unnumbered** VSAs have the following syntax:

```
Cisco:Cisco-AVpair = "ip:vrf-id=vrf-name"
Cisco:Cisco-AVpair = "ip:ip-unnumbered=interface-name"
```

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

Whenever you specify a VRF in a user profile, but you do not configure the VRF on the Cisco 10000 series router, in Cisco IOS Release 12.2(15)BX, the router accepted the profile. However, in Cisco IOS Release 12.2(16)BX1 and later releases, the router rejects the profile.

Setting VRF and IP Unnumbered Interface Configuration in a Virtual Interface Template

You can specify one VSA value in the user profile on RADIUS and another value locally in the virtual template interface. The Cisco 10000 series router clones the template and then applies the values configured in the profiles it receives from RADIUS, resulting in the removal of any IP configurations when the router applies the profile values.

Redefining User Profiles to Use the `ip:vrf-id` and `ip:ip-unnumbered` VSAs

The requirement of a full virtual access interface when using the `lcp:interface-config` VSA in user profiles can result in scalability issues, such as increased memory consumption. This is especially true when the Cisco 10000 series router attempts to apply a large number of per-user profiles that include the `lcp:interface-config` VSA. Therefore, when updating your user profiles, we recommend that you redefine the `lcp:interface-config` VSA to the scalable `ip:vrf-id` and `ip:ip-unnumbered` VSAs.

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

Example 1 *Redefining VRF Configurations*

Change:

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

To:

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

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

Example 2 *Redefining IP Unnumbered Interfaces*

Change:

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

To:

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

Inserting a New Line Card

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

Provisioning for Scaling

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

- [PPPoA Sessions with IP QoS Static Routes, page 13](#)
- [AAA Authentication on the NME Port, page 13](#)
- [Call Admission Control, page 13](#)

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

For more information, 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 NME port, set both the in and out interface hold queues to 4096; for example:

```
Router(config)# int fa 0/0/0
Router(config-if)# hold-queue 4096 in
Router(config-if)# hold-queue 4096 out
```

Call Admission Control

We recommend that you set the Call Admission Control (CAC) to a maximum of 95; for example:

```
Router(config)# call admission limit 95
```

Caveats for Cisco IOS Release 12.3(7)XI8

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

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

All caveats in Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T that apply to the Cisco 10000 series are also in Cisco IOS Release 12.3(7)XI8.

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](#).



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](#) and click **Products and Services: Cisco IOS Software: Cisco IOS Software Releases 12.2: Troubleshooting: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have

requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

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

Open Caveats—Cisco IOS Release 12.3(7)XI8

This section describes caveats that are open in Cisco IOS Release 12.3(7)XI8.

- 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 not getting updated/displayed correctly.

There are no known workarounds.
- 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: Lowering configured speed to 9999Kbps will 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 4-5 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.

- CSCec86624

Traffic convergence after the removal of APS on line card 1-Port Channelized OC12, was greater than 2 sec.

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 utilization is detected for 5 minutes after unconfiguring half-duplex VRF with a large number of PPPoE user sessions. This problem occurs with 32,000 PPPoE sessions therefore, scaling to high values.

There are no known workarounds.

- CSCed72338

The system allows non-nested queuing policy maps to be applied 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:

1. 4,095 VRFs are configured on a router
2. 500 eBGP sessions are established between the router (PE) and CE routers
3. 540 VRF routes per VRF in the 500 VRFs that are running eBGP between PE and CE routers
4. 40 VRF routes per VRF in the rest of 3595 VRF

There are no known workarounds.

- CSCee06089

When you apply a nested policy map using the **bandwidth** command in the child policy map to a POS 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 no cdp run.
- 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 **protocol pppoe** and **dbns enable** (Dynamic Bandwidth Selection).
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 subrates 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, tracebacks can occur when an ATM VC is deactivated.

There are no known workarounds.
- CSCef20523

PPPoEoA sessions using CBWFQ experience BQ drops. In some cases, when aggregate traffic is near the VC rate, the BQ tail drops packets. This problem appears with low bandwidth VCs, in this case 196 kbps.

Workaround: Changing the queue-limit 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.

- CSCef47280

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

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

There are no known workarounds.
- CSCef47688

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

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

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

There are no known workarounds.
- CSCef50661

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

Workaround: Both the weight and queue depth can be configured with CLI. Ensure that the queue depth is at least as high as the weight.
- CSCef51082

The discard bit match is not done at the MPLS output interface when it is set at the VRF input interface. This problem occurs when the qos set was initially done with the mpls exp bit, then changed to the discard bit.

Workaround: If the discard bit needs to be matched at the MPLS interface, do not configure the mpls exp bit set at the VRF input interface.
- CSCef56348

With PPPoE, PPPoA, or VPDN sessions, the following message may appear in the log: “*Aug 25 06:57:07.759: Reload unknown session type.” This problem can occur after a microcode reload.

There are no known workarounds.
- CSCef56455

On rare occasions, configuring speed using the Dynamic Bandwidth Selection (DBS) feature is not fully reliable. Initial user connections are properly set, but subsequent connections will not. This failure to configure the connection speed using DBS occurs when bringing up over 2,000 user connections.

There are no known workarounds.
- CSCef59264

The IP shaping rate is changed to the VC shaping rate provisioned 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)XI1 can reload unexpectedly. Output similar to the following is displayed on the console during the reload:

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

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

There are no known workarounds.

- CSCef71570

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

There are no known workarounds.

- CSCef72129

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

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

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

There are no known workarounds.
- CSCef74370

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

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

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

There are no known workarounds.
- CSCef75434

Inaccurate traffic counters are displayed when running traffic on the Managed LNS router. Cisco 10000 series LNS routers do not match the transmit and receive packets for Managed LNS traffic.

There are no known workarounds.
- CSCef76338

PTA PPPoE 8,000 PVC 32,000 queue, send mixed size line rate traffic, packets drop. Condition: Send mixed size packets line rate traffic, packets tail drop on BQ.

Workaround: Lower the traffic rate.
- CSCef79045

The auto VCs (infinite range VCs) do not disappear even when the traffic from the client is stopped. If traffic is sent on a large number of VCs at a high rate, then infinite range VCs are created, they do not disappear even when the traffic is stopped or the interface is shut down.

Workaround: Stop the traffic and wait for a couple hours for the buffer to clear up and then eventually the VCs to disappear or reload.
- CSCef79688

MPLS Packets are punted to the Route Processor. This problem occurs when MPLS Packets are sent over a Frame Relay Interface.

There are no known workarounds.

- CSCef80176

If a user has a `vbr-nrt vc` configured within a `vpv` 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 will try to execute on the leftover VAI and will lead the router to stop responding.

Workaround:

1. Change `vbr-nrt` parameters using `vbr-nrt new_pcr new_scr new_mbs` command.
2. Avoid deleting `vbr-nrt` service configuration from a VC which is configured within 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)X11, 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)X12 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)X12, 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 is sent out in authentication requests, based on what the configuration on the router was for the same. This problem occurs when the per-server group nas-port has been configured on the Cisco 10000 series router in such a way that the nas-port value in all authentication requests should be sent out in format e string of 32 I's (VPI value of incoming session) and the accounting requests should be sent out in format e string of 32 C's (VCI value of incoming session). However, on session bring up the authentication requests have a nas-port value representing the format e string value corresponding to 32 C's, which is incorrect.
 There are no known workarounds.
- CSCef93639
 Some Multilink PPP member links turn to up/down after an MR-APS switchover. This problem occurs with T1 interfaces over 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 Utilization than normal when configuring it with VRFs with VPN overlay. This problem occurs while attempting to bring up 645 PPPoA sessions over 215 VRFs (with VPN overlay) and there are approximately 150,000 BGP routes in the system.

There are no known workarounds.
- CSCef94504

Cisco 10008 router can reload when reporting a software forced crash (memory corruption). The problem was reported in 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: Do **no ip domain server lookup**.
- CSCef95719

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

There are no known workarounds.
- CSCef95738

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

Workaround: The only changeable parameter is the keepalive; turning it off or changing the value to a larger one might improve the situation.
- CSCef95814

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

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

There are no known workarounds.

- CSCef97118

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

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

- CSCef97194

OC-12POS 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 aal5ciscoppp 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 aal5ciscoppp.
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 utilization 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 utilization is rising to 100 percent (or close) and causing other active sessions to be disconnected. Active sessions being disconnected is also due to the inability of the Route Processor to handle the sending and receiving of the PPP keepalive on these active sessions. The reload is causing an RP switchover but the new active RP is logging the following error messages continuously:

```
Oct 14 17:03:32.401: %C10K-4-LC_WARN: Slot [8/0] 1oc12atm-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] 1oc12atm-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 **sh run** 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.
- CSCeg48971
 The command to display cached PPPoE configuration information is present in Cisco IOS 12.3T images, but not in Cisco 12.3(7)X13. The command which is affected is **show pppoe derived**.
 There are no known workarounds.
- CSCeg56821
 The link should be DOWN between UUT & HP37718 for Frame format pcm31 & crc4.
 The test involves three sub tests.
 (1) Valid Frame Format Combinations -- CRC4(E1) or SF(T1)
 (2) Valid Frame Format Combinations -- NO CRC4 (E1) or ESF (T1)
 (3) Invalid Frame Format Combinations -- pcm31 crc4
 The first two sub tests passed. Only third sub test is failed. In the third sub test, invalid frame combinations are configured, and the link should be down once it is configured. But here the link is up.
 There are no known workarounds.
- CSCeg61244
 Template down loading may not work with [CSCee52915](#) feature. 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.

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


To add a new class with Priority I lost ACTIVE PRE to software crash.
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
Packets 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
Symptom: 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 31.5K sessions over 2 OC-12ATM 31500 subinterfaces, only 29k sessions up after 30 min, 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 2 OC-12ATM 31.5000 subinterfaces, with input police PMAP in virtual-template, and output 3 queue PMAP, 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 OC48POS 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)X13, 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 VAI's 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 ACL's are generating a high CPU after a reload.
Workaround: Configure MINI ACL's (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.

 - CSCei49897

PXF Queues of VBR VCs are removed.

Workaround: Delete the VC and recreate VBR VCs with the new values.
 - 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 dbs 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

"bandwidth X kbps" or "bandwidth percent X %" and "bandwidth remaining percent Y %" are configured for a traffic class.. and when I unconfigure "bandwidth remaining percent Y %".. "bandwidth X kbps" or "bandwidth percent X %" is being removed from running config than "bandwidth remaining percent Y %".

Workaround:

Unconfigure "bandwidth remaining percent Y %" for the second time and configure the "bandwidth X kbps" or "bandwidth percent X %" which was removed from the running config in the first unconfiguration of "bandwidth remaining percent Y %"
 - 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 12-3(7)XI5 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
1. Unconfigure & configure child policy map in a nested service policy with different parameter for police action (here BURST) has no effect.
2. Assertion failure seen during the **show policy-map int** command execution and the output has no police statistics.
Workaround: Unconfigure and configure the policy map under GigE sub interface
- 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 crash is observed in post router check.
There are no known workarounds.
- CSCej01828
Wrong I/P & O/P Packet count in the output of "show interface FULL/BASE VAI (or) SUB VAI (or) 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 Cisco10000 series router experiences PXF crashes with the 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 12.2(XI) release HH-CHT3 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 the **no card type** configuration.

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 12.3(7)X16 subscribers, using the PPPoE TAG feature, wait for more than 20 secs 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 will discard 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) before sending again that LCP REQ.

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) will cause 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 will stop 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.
- CSCej75389

On a mutli link 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 pervrfaaa config, 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 tracebacks and error messages while running configuration of PPPoEoA and DBS (Dynamic Subscriber Bandwidth Selection) and moderate downstream traffic. Some PPPoEoA sessions may fail to bring up because of that. The message and error look like these:

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

There are no known workarounds.
- CSCej76195

Cisco 10000 series router is experiencing spurious accesses while running PPPoEoA, DBS (Dynamic Subscriber Bandwidth Selection) and moderate downstream traffic.

There are no known workarounds.

- CSCej76827

Traceback observed when **ipc_send_rpc_blocked** command failed.

There are no known workarounds.

- CSCej76986

dsx3LineType does not match the CLI obtained value

There are no known workarounds.

- CSCej76995

Idle timeout brings the AutoVC down in presence of 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 TurboACLs with SSG sessions. Instead, use miniACLs, 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 miniACLs.

- CSCek01900

show policy-map int <sub vai> shows junk stats for few sessions.

Execute **clear counter CLI** after ucode reload.

- 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 when ATM LC OIRd.
There are no known workarounds.
- CSCek04301
Impossible serial interface counter statistics.
There are no known workarounds.
- CSCek11664
A forwarded packet may be lost on a PPPoE session on a Cisco 10000 series router.
There are no known workarounds.
- CSCek17507
Implement the vtemplate cancel API.
There are no known workarounds.
- 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.
- 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 PPoE after we remove the previously configured "bba-group" for PPoE, the **protocol** command in the VPDN accept-dialin configuration mode does not allow the "PPPoE" option.

Workaround: Before removing bba-group, 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 (sub)interface or pvc specification - the subordinately defined bba-group references must 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-record 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.
- 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 will be 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 transitting a policed PQ on the LAC are dropped.

Workaround: Increasing the policed bps rate within the PQ lessened the drops somewhat but could 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 command **show controller atm x/y/z**.
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 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 crash 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" action 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
ATM-3-FAILREMOVEVC: ATM failed to remove VC message followed by %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 during downgrade from 12.2.SBB to 7XI5.
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 interim image based on 12.3(07)XI. Router shows the following align 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__FPvUI

- There are no known workarounds.
- CSCsb55246

PXF crash 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.
 - CSCsb57122

On a PRE-2 the following message Shape rate too low for GigabitEthernetXXX May be displayed, even with a valid shape rate value

Workaround: Use nested policy-map to avoid the message.
 - CSCsb59396

Cisco 10000 series router with 12.3(7)X12a based version 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 may see the following message on the console or log:

```
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 box.

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 show policy-map interface 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

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

There are no known workarounds.
 - CSCsb66252

When running multiple instances of "show pxf cpu queue ATM x/y/z" whilst del/adding service policys and overwriting the vc-class on many PVC's it is possible the Cisco 10000 series router may stop responding with a bus error.

There are no known workarounds.
 - CSCsb68306

PRE2 PXF is stops responding with PXF DMA TBB Length Error.

There are no known workarounds.

- CSCsb78535

A Cisco 10000 router may show the following log message: c10k_l2tp_hw_session_open: not able to retrieve vcci.

There are no known workarounds.

- CSCsb79060

Random T1's in a CHOC3 Line card are sending LOF. The result is that the T1 is down/down.

Workaround: Reloading the Line Card with the **hw-module slot x reset** command should restore normal operation.

- CSCsb79666

If a new Cisco 10000 series router 6 Port OC3 line card is inserted into a Cisco 10000 router and then Encapsulation HDLC is configured, the POS interface would not send out any Keepalive packets. The **show interface** command would not display 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 w/31000 PPPoEoQinQ sessions up.

There are no known workarounds.

- CSCsb88950

When terminating PPPoE clients on a Cisco 10000 router running 12.3(7)X15, 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 was reported when establishing PPOA/PPPOEOA sessions with an associated output service-policy.

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
A Cisco 10008 router may suffer PXF non response with the following message:
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
PRE2 PXF is not responding with PXF DMA TBB Length Error.
There are no known workarounds.
- CSCsc08516
Sep 30 06:45:35.727: %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=63EA6E34, count=0 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.
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 during downgrade from 12.2(27-7.29).SBB1 to 12.3(7)XI6. Traceback messages:
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 being disconnected after idle-timeout
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 enable cdp under interface.
There are no known workarounds.
- CSCsc22473
A Cisco 10000 series router stops responding due to the **turbo_acl_process** command when running 12.3(7)XI2b
There are no known workarounds.
- CSCsc22692
Amount of free processor memory decreases every day. PPPEvents process is slowly taking all the memory without freeing memory. This happens on a Cisco 10000 series router running 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 OC3 or OC12 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 stop responding and indicates: %PXF-2-FAULT:
There are no known workarounds.
- CSCsc33012

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

There are no known workarounds.

- CSCsc33334

PRE stop responding while collecting some policy map related counters.

There are no known workarounds.

- CSCsc33381

PPP: tracebacks found when applying per user attributes

Workaround: None. 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 utilization cause active PRE2 switch-over 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 BTS (Base Transceiver Station). If a T1 is active over each Cisco 10000 series router the BTS reloads due to losing communications with the RNC (Radio Node Controller) which 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 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 utilization.

There are no known workarounds.

- CSCsc42659
on-demand VC stuck after PRE2 switchover if set atm idle-timeout is set to 1.
There are no known workarounds.
- CSCsc42985
Cisco 10000 series router, running 12.3(7)XI5, may stop responding when change "police percent" value of 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 still busy after clear line vty is given.
There are no known workarounds.
- CSCsc48355
Router IOS stops responding.
Workaround: Do not change policy-map and queue-depth repeatedly.
- CSCsc49599
After clearing PPPoE sessions, the sessions are not seen anymore in the **sh pppoe sum** command as expected but they are seen in the **sh sss sessions** command.
There are no known workarounds.
- CSCsc51423
Both MR-APS ports report Active.
Workaround: Force an MR-APS cutover using the **aps force** command or **shut/no shut** command on one of the MR-APS interfaces.
- CSCsc51520
Mismatch between IOS 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 more than 8 rules long 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
Active PRE2 switch-over -- atm_get_idle_timeout_params.
There are no known workarounds.
- CSCsc60017
After PRE2 switch-over shut/noshut cause on-demand range vc become INAC.
There are no known workarounds.
- CSCsc61178
The **show redundancy state** and **show redundancy** commands on Cisco 10000 series routers running 12.3(7)X16 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.
- CSCsc63969
Cisco 10000 series router - LI - Fragmented packet (2nd fragment) not tapped.
There are no known workarounds.
- CSCsc65489
System stops responding in DMA stats collector.
There are no known workarounds.
- CSCsc65624
Static ATM VC becomes INAC after hw-module reset --- exist VCCI.
There are no known workarounds.

- CSCsc65655
System non-response observed in Micro_get_block.
There are no known workarounds.
- CSCsc66947
MRAPS: Shut on W interface causes P router console to stop responding.
There are no known workarounds.
- CSCsc69861
Service Selection Gateway: Send VSA 9.2 for IPoQinQ, 9.2 for PPPoE
There are no known workarounds.
- CSCsc69892
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 counter are not displaying correctly on FULL VAI.
There are no known workarounds.
 - CSCsc83269
PXF CEF values change causing packet loss.
Workaround: Shutdown the redundant path.
 - CSCsc91155
A Cisco 10000 series router 12.3(7)XI7 image crash generated the following error:
%C10K_QUEUE_CFG_GENERAL-2-EREVENT
There are no known workarounds.
 - CSCsd36790
A traceback is observed 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.
 - CSCse57404
A router running IOS 12.3(7)XI7 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.
 - CSCse58444
The 4-Port Channelized OC-3/STM1 line card stops transmitting packets. The output of the FIB registers on the line card show all FPGA buffers are depleted.
Workaround: A reload of the 4-Port Channelized OC-3/STM1 line card will restore service.
 - CSCse58765
A Cisco 7200 router with NPE-G1 may crash 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 crash when configuring 1-Port Channelized OC-12 line card.

There are no known workarounds.

- CSCse60811

PRE2 crash related to QoS config policy-map change.

There are no known workarounds.

- CSCse61797

A class VC may stop passing traffic and generate 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 crash during LCP session cleanup.

There are no known workarounds.

- CSCse64787

A policing service-policy is not applied to PPPoE (oQinQ) L2TP forwarded sessions. This was observed in a Cisco 10008 router PRE2.

Workaround: Reapply the service-policy to the Gigabit Ethernet subinterface after the PPP session is established.

- 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

Crash while churning security turbo ACLs in IOS 12.3(7)X17.

There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(7)XI8

This section describes caveats that were fixed in Cisco IOS Release 12.3(7)XI8.

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

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

- CSCdv66525

A Cisco 10000 series edge services router may not produce a Parallel Express Forwarding (PXF) error message after a PXF engine has reloaded unexpectedly.

There are no known workarounds.
- CSCea60973

A T1 interface may flap on the near end and the remote end.

There are no known workarounds.
- CSCeb05456

A sup720 may reset the Route Processor when two simultaneous 'wr mem' from two different VTYS has performed.

Workaround: Set the boot config, if supported, to non nvram medi, such as disk, bootflash.
- CSCeb13473

Not able to configure more that 128 channels per AU4TUG3. Following error message is observed:

```
%T1 (tug-2 1 t1 1) channel group 20 can't be configured because exceeding max. 128 channels
%Insufficient resources to create channel group. Configure more than 128 channels on one
AU4TUG3
```

Workaround: In order to reach the 192-channel per/STM1 limit, configure the other channels on another AU4TUG3 on the same STM1.
- CSCeb27812

A Cisco 3660 router may have a memory leak in the crypto Internet Key Management Protocol (IKMP) process after repeated attempts are made to connect to the Certificate Authority (CA) server that holds the certificate revocation list (CRL).

There are no known workarounds.
- CSCec629933

The following error message is seen with 'debug vpdn l2x-errors' enabled when users are trying to connect to an LNS: vpn_set_ppp_remote_name: Error inserting username, user@domain, into String DB Where 'user@domain' is the username and domain being used to connect with.

Workaround: This message is only seen when debugging vpdn l2x-errors. It appears to be only cosmetic in nature.
- CSCed00033

When an ATM PVC bounces, it fails to come back up and remains in the DOWN/UNVERIFIED state.

Workaround: Reactivate the PVC by entering the **shutdown** command followed by the **no shutdown** command on the PVC or disable OAM management.
- CSCed15056

High CPU usage at process = PPP IP Route and router reloads. The Symptoms are observed on a Cisco 7200 and RSP series running IOS 12.3(4)T1 image.

There are no known workarounds.

- CSCed22200

The router does disconnect the call specified in PoD correctly, but in its acknowledgement response to RADIUS server the source IP address is the one of the outgoing interface, rather than the one specified with **ip radius source-interface** command.

All other RADIUS packets sent by the router use IP source as specified in **ip radius source-interface** command correctly.

There are no known workarounds.

- CSCed29494

The maximum queue size for low speed link changed to 4096 instead of 8192, the ios accepts queue-limit 8192 command, but set it to 4096 without error message.

Workaround: Set maximum queue size to 4096.

- CSCed64702

On a Cisco 10000 series router, the PXF information may not be correctly updated from the Route Processor after a route change, causing packets to be sent untagged even though the Route Processor shows that the packets should be sent as tagged.

Workaround: Enter the **clear isis *** command or enter the **shutdown** command followed by the **no shutdown** command on the interface towards the MPLS cloud.

- CSCed86286

A router may reload due to a software-forced crash.

There are no known workarounds.

- CSCee19119

Connected routes are erroneously installed over interfaces configured for PPP encapsulation that have not negotiated the PPP IP Control Protocol (IPCP). This can result in IP packets being discarded when they are mistakenly switched over such interfaces. Debug messages such as "PPP: Outbound ip packet dropped, NCP not negotiated", "IP: s=a.b.c.d (local), d=e.f.g.h (Serial3/2), len 100, encapsulation failed.", and/or "MLP: ip packet forwarded to wrong interface" may be displayed if the **debug ppp negotiation**, **debug ip packet**, and/or **debug ppp multilink event** commands are entered. This symptom is observed when an IP address and subnet mask are configured on an interface, and that interface subsequently comes up without negotiating IPCP, either because the peer rejects the protocol or because the interface joins a PPP Multilink bundle (in which case IPCP is negotiated on the bundle interface).

Workaround: Either configure **no ip address** or **ip unnumbered** on the interface, rather than configuring an IP address and suGbnnet mask.

- CSCee37501

Open Shortest Path First (OSPF) can lose neighbors (if fast hellos are configured) after a **write memory** command is issued on a router.

There are no known workarounds.

- CSCee42865

When **ip radius source-interface int** is configured, then PoD response will be sent with wrong IP source IP address.

- There are no known workarounds.
- CSCee55457

When a channel group (for example, channel +1) is removed from a controller, the class-default queue gets stuck on the next time slot/channel.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.
 - CSCee55828

You cannot configure **t1 1 framing esf** and **t1 loopback remote** at the same time on a 1-port channelized OC-12 line card. This problem occurs when you configure **t1 1 framing esf** under an AU-4 on a 1-port channelized OC-12 line card.

Workaround: Configure **t1 1 framing esf** without the loopback configured for the T1.
 - CSCee57686

TU controller on the 4-port channelized OC-3 line card does not go down when a RDI alarm is received.

There are no known workarounds.
 - CSCee62326

A router configured for MPLS tag-switching may generate the following message intermittently: %TFIB-7-SCANSABORTED: TFIB scan not completing.

There are no known workarounds.
 - CSCee68905

An extensible authentication protocol-subscriber identity module (EAP-SIM) user cannot log off and reconnect when PBHK is enabled.

There are no known workarounds.
 - CSCef09119

With broadband PTA 128,000 queue with input and output policy map, removing the input policy from Virtual-Template causes a high CPU usage traceback message. This occurs when configuring 31.5,000 ATM subinterfaces with output CBWFQ policy, and input police policy in Virtual-Template, bringing up 30,000 PPPoE sessions, and removing the input policy map.

There are no known workarounds.
 - CSCef29091

Symptoms: A router may fail to advertise a prefix for which the network portion matches the major net. For example, when 10.0.0.0/8 is the major net, 10.0.0.0/16 is not advertised.

Workaround: On the advertising router, enter the **shutdown** command followed by the **no shutdown** command on the interface that is connected to the receiving RIP peer.
 - CSCef29506

The first time the IS-IS routing protocol is enabled on some interfaces, it may not form the appropriate neighbor adjacencies if those interfaces are enabled with the IP Event Dampening feature, identified by the configuration:

```
interface <>
dampening ...
```

Workaround: Issue the command **shutdown** and then **no shutdown** for that interface.

- CSCef73233
 Commands parsed when doing **copy ftp: running-config** are applied correctly to the config, but they do not show up in the tacacs log when tacacs+ accounting has been enabled. Same commands do show up in log when executing them using CLI.
 There are no known workarounds.
- CSCef58522
 Almost every hour the following error message is generated: %TFIB-7-SCANSABORTED: TFIB scan not completing. Unresolved adjacency.
 There are no known workarounds.
- CSCef81634
 Using the external generating tool IXIA Explorer to bring up and tear down SSG sessions quickly, the PRE2 stop responding with a Bus Error Exception. This problem occurs when the tool initializes the interface and quickly brings sessions back up while the old sessions are still cleared out.
 There are no known workarounds.
- CSCeg00438
 On a Cisco 10000 series router running Cisco IOS Release 12.3(7)X11, the policer counters in the output of **show policy-map interface** do not increment if the policy map is applied to a Virtual Access Interface. The police conformed/exceeded/violated counters are not updated (values are all zeroes) when an output service policy is applied on a virtual- access interface.
 There are no known workarounds.
- CSCeg11451
 A Cisco platform that functions as a MPLS VPN provider edge (PE) router that is configured as a multihop LNS and that switches L2TP tunnels from the global routing table into a customer VRF may select an incorrect VRF table to send the L2TP control packets to the customer LNS.
 There are no known workarounds.
- CSCeg53851
 Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0S or interim Release 12.3(12.8).
 There are no known workarounds.
- CSCeg72444
 A router that is configured for SSG may hang and stop responding.
 Workaround: Disable idle timeout for all PPP users.
- CSCeg75974
 A router sends a SSG Prepaid authorization requests to the AAA server instead of to the SSG Prepaid server.
 Workaround: Do not configure the SSG Prepaid server via the PZS attribute in the local SSG Service profile but manually configure the SSP Prepaid server by entering the following commands:

```

aaa group server radius server-group-name
server ip-address
auth-port auth-port
acct-port acct-port
ssg aaa group prepaid server-group-name
    
```
- CSCeg80079

Large ping packets destined to the Cisco 10000 series router fail.

Workaround: Send smaller ping packets.

- CSCeh06778

If a default route is redistributed from RIP into BGP, then back into RIP on another router, the default route is not marked as poisoned or withdrawn on the CE router that receives the updates.

There are no known workarounds.

- CSCeh11771

On a leased line (non-dialup) serial connection that is configured for PPP encapsulation, the line protocol may not come back up when the connection is reset. The PPP LCP remains in the closed state, even though the link is up physically.

There are no known workarounds.

- CSCeh30577

OC-12 ATM interface shows incorrect available bandwidth = 149760 Kbps in show atm interface atm x/y/z while no PVCs/PVPs are configured under this port. This symptom is observed in Cisco's 10000 series router running on 12.3(07)XI IOS image. Due to this, once PVCs/PVPs are configured more than the available bandwidth = 149760 Kbps, the CLI **show** command mentioned above will start showing the Link oversubscribed. But it should not show link oversubscribed until configured bandwidth cross 599040 Kbps for OC-12 ATM.

There are no known workarounds.

- CSCeh45997

NAT translated packets are updated in miss counter in "show ip nat statistics" output.

There are no known workarounds.

- CSCeh50583

Cisco 10000 series router configured for SSG may send wrong NAS-Port and Accounting session ID in connection accounting records. This happens when the access type is PPPoEoQinQ.

There are no known workarounds.

- CSCeh61836

SSG wrongly sends the attribute QR0 in a re-authorization request after it has received a quota combination of QT>0,QX=TS>0;PRE>0;POST=0,IT=0 from Prepaid Server for tariff switch case.

Workaround: QR0 should only be sent after getting the TS quota combination of QT>0,QX=TS>0;PRE=0;POST=0,IT=0 and after the QT expires.

- CSCeh65480

Repeated attachment of a bogus class does not give any feedback. Attach a bogus VC class to an ATM VC repeatedly.

There are no known workarounds.

- CSCeh73049

Symptoms: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (TCL) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

Conditions: Devices that are not running AAA command authorization feature, or do not support TCL functionality are not affected by this vulnerability.

This vulnerability is present in all versions of Cisco IOS that support the **telsh** command.

Workaround: This advisory with appropriate workarounds is posted at

<http://www.cisco.com/warp/public/707/cisco-response-20060125-aatcl.shtml>

- CSCei00766
A router may crash when the encapsulation is set to PPP and removed repeatedly.
There are no known workarounds.
- CSCei03036
OAM flush drives CPU interrupt utilization high.
There are no known workarounds.
- CSCei05511
Progress filed is not accurate in the accounting packet, it shows "No progress".
There are no known workarounds.
- CSCei05676
If CDP is enabled or disabled on a Cisco 10000 series router HH-1GE interface, the interface goes down and back up again. This results in an interruption of traffic for up to 5 seconds.
There are no known workarounds.
- CSCei11909
After the default VPDN group has been chosen in the configuration, this choice is not revised irrespective of the subsequent configuration changes:
* If another vpdn-group [displayed in IOS configuration above the original default group] is [also] configured to act as default, this new default group is ignored.
* If the original default group stops being the default (e. g., "terminate-from" is configured under it), the LNS still attempts to terminate the subsequent VPDN calls intended for the default vpdn-group under the same group as before.
Because of the configuration changes these calls may start failing, instead of being redirected to another suitable vpdn-group.
Workaround: Reloading the router returns the behavior to normal.
- CSCei16649
The output of the **show pppoe session** or **show vpdn session** command does not show PPPoEoA session details.
There are no known workarounds.
- CSCei17730
Long Single Sign-On (SSO) switch-over times is experienced when using 4 Port Channelized OC3 and Channelized OC12 line cards.
There are no known workarounds.
- CSCei20806
Stateful switchovers to the redundant RP can take longer after the configuration of the interface encapsulation on the Channelized OC3 or OC12 line cards have changed. After the cutover it can take 60 seconds or longer for full traffic to resume.
There are no known workarounds.

- CSCei21744
When 31000 PPPoE established over 31,000 QinQ subinterfaces, the processes like bringing sessions down when the port goes down, pxf microcode reload, HA takes 99%-100% of cpu. As a result, when the physical port goes down it takes about 5 minutes for all sessions to go down. Another problem is, it takes about 4 minutes to reload PXF microcode, and most of the sessions are getting disconnected. HA takes about 5-7 minutes.
There are no known workarounds.
- CSCei46572
A bus error crash may happen on Cisco 10000 series router while changing ATM traffic shaping on the live sessions repeatedly.
There are no known workarounds.
- CSCei47316
Spurious memory access with WRED configured in user-defined class without queue.
Workaround: Do not configure WRED in a traffic class without queue.
CSCei47703
High CPU usage due to diverted packets encap reason on Cisco 10000 series router.
There are no known workarounds.
- CSCei55409
PRE2 stops responding unexpectedly without any config or hardware change.
There are no known workarounds.
- CSCei60741
Traffic path from PTA(Cisco 10,000 series router) to EDSLAM is broken for user defined traffic classes in the PPPoEoVLAN session as the user defined PXF queues of the session are removed.
Workaround: Unconfigure the child policy map from the parent policy map of the nested service policy and configure it again using **no service-policy child policy name** and **service-policy child policy name** configuration commands.
- CSCei62952
After a PXF stops responding, certain prefixes are no longer routable.
Workaround: Reboot the route processor.
- CSCei63369
When a single router-APS (SR-APS) is configured Channelized/STM1 line cards on Cisco 10000 series routers, resetting or Online Insertion and Removal (OIR) of one card will stop the traffic, and it will not restart.
Workaround: To clear the symptom, remove APS configuration by entering the **no associate slot slot_one slot_two** command and then, re-configuring APS by entering the **associate slot slot_one slot_two** command.
- CSCei76015
Traceback is observed after loading the image and when the toaster is getting initialized.
There are no known workarounds.
- CSCei83838

It takes too long for traffic to resume after an HA switchover on a 4 Port Channelized OC-3 line card on a Cisco 10000 series router.

There are no known workarounds.

- CSCei84416

A 4-Port channelized OC-3 line card resets unexpectedly.

Workaround: Ensure that the correct clocking is configured.

- CSCej00097

Interfaces on the Cisco10000 series router 1 Port Channelized OC12 port may take too long to recover after a PRE switchover.

There are no known workarounds.

- CSCej00366

The ifType for ATM OC-12 interfaces are shown as other(1) in SNMP MIBS ifTable

There are no known workarounds.

- CSCej01612

"clear counter" does not reset packet counts in "show interface full vai" output to ZERO. Execute "clear counter" after the session bringup.

There are no known workarounds.

- CSCej12324

A Cisco 10000 series drops a packet for a prefix with an incomplete CEF adjacency.

Workaround: Send a ping for the prefix with the incomplete CEF adjacency in order to complete the CEF adjacency.

- CSCej26464

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

There are no known workarounds.

- CSCej28138

Buffer low drops are not accounted as drops in the output of

show int main interface

show int SUB VAI

and

show pxf cpu queue SUB VAI commands.

There are no known workarounds.

- CSCej28162

Tail drops are not accounted for in the output of **show int main interface** command. Tail drops happened when the system limitation for packet handles is reached.

There are no known workarounds.

- CSCej28291

Low link utilization at a throughput of about 70 percent may occur in certain configurations and traffic patterns.

There are no known workarounds.

- CSCej35046
After a PXF stops responding, the PFX does not get reloaded. This is caused by 2 PXF stop responding back-to-back. The second PXF stop responding causes the PXF reload to be incomplete.
There are no known workarounds.
- CSCej43295
A traffic interruption of over 20 seconds occurs when fiber is pulled from a port in an SR-APS configuration.
There are no known workarounds.
- CSCej44508
Cisco 10000 series router stops responding during MR-APS switch over
There are no known workarounds.
- CSCej45787
Router acting as PPPoE over ATM server could stop responding.
There are no known workarounds.
- CSCej60234
PPPoE running BRAS could run into alignment errors while reading incoming data frame.
Workaround: The system recovers by itself.
- CSCej70228
Netflow not working with the older command, ip route-cache flow.
There are no known workarounds.
- CSCej75636
Configuration not properly loaded after reboot.
When reloading the Cisco 10000 series router, it looks like the startup configuration is not being parsed correctly.
There are no known workarounds.
- CSCek01717
Tracebacks seen when **pppoe_common_cleanup** command is called from the **validate_pad** command.
There are no known workarounds.
- CSCek05853
Datagram size needs to be re-adjusted after stripping off tag.
There are no known workarounds.
- CSCek21636
PPPoE Circuit-Id Tag: Feature does not work in IOS 12.3(7)X17.
There are no known workarounds.
- CSCek27756
All interfaces flap on a 24-Port Channelized E1/T1 line card.
Workaround: Microcode reload followed by card reset.

- CSCek29813
The controller on the OC3ATM/OC12ATM line card is down with no alarms indicated.
Workaround: Reset the line card.
- CSCek37177
The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.
This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.
Cisco has made free software available to address this vulnerability for affected customers.
This issue is documented as Cisco bug ID [CSCek37177](#).
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-20070124-crafted-tcp.shtml>
- CSCin75131
The memory in use may increase over time. This condition is observed on a Cisco router that has active SSG tunnel services and users that are logging into and logging off the tunnel services.
There are no known workarounds
- CSCin79875
A spurious memory access may occur on a Cisco router that is configured for PPPoA. This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(10.3).
There are no known workarounds.
- CSCin80523
A router that runs Service Selection Gateway (SSG) may reload.
There are no known workarounds.
- CSCin86689
Auto VCs on the DOWN interface remain INACTIVE.
Workaround: Shut/no shut the main interface. This will force the PVCs to be properly torn down and recreated in the new configuration.
- CSCin87258
A Cisco router that is configured for SSG may reload when you configure a local service profile.
There are no known workarounds.

- CSCin87464
A spurious memory access occurs on an SSG when you run a MIB get request for the SSG service binding entries.
There are no known workarounds.
- CSCin87560
The following error message is displayed on a router that is configured for SSG:
%SYS-3-BADLIST_DESTROY: Removed a non-empty list
Workaround: Before you unconfigure the SSG feature, unbind the SSG service by entering the **no ssg bind service** *service name/ipaddress/interface type/interface* command.
- CSCin91267
You may not be able to bind interfaces to an uplink or downlink if your system is configured for SSG.
There are no known workarounds.
- CSCin96611
SSG does not send NAS port ID on access request for service with prepaid quota.
There are no known workarounds.
- CSCsa44720
A Cisco router may reload unexpectedly with a bus error exception. This symptom is observed on a router that is configured for Service Selection Gateway (SSG) and authentication, authorization, and accounting (AAA).
There are no known workarounds.
- CSCsa45029
The interface bandwidth shown under the virtual-access interface is not reflecting the right BW value. This typically happens when the interface's VC is reconfigured using DBS. The BW value should adjust to the ATM SCR as specified in the DBS parameters. PPPoX and use of DBS. This behavior is only seen when DBS is reconfiguring the VCs BW/SCR.
There are no known workarounds.
- CSCsa50533
On a Cisco 10000 series GE card 30 second output rate may fluctuate. Large number of interfaces configured on the system.
Workaround: Configure 5 minute load interval.
- CSCsa52807
A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).
These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:
 1. Attacks that use ICMP "hard" error messages
 2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

3. Attacks that use ICMP "source quench" messages.

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

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

Workaround: Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>

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

- CSCsa53909

The **aps manual** command switches traffic to DOWN interface causing all traffic to be lost.

Workaround: Use **aps-force** command Instead.

- CSCsa57203

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

There are no known workarounds.

- CSCsa58396

The Cisco 10000 series router may display the "C10KEVENTMGR-1-IRONBUS_FAULT: Barium Error" error messages on some of the line cards when switching from the Active to the Standby PRE.

There are no known workarounds.

- CSCsa62475

When a PPP user with a SSG ACL defined in his RADIUS profile disconnects the PPP session, alignment error is seen.

There are no known workarounds.

- CSCsa65096

A router may stop responding during the boot process when the startup configuration includes the **hw-module shutdown** command.

There are no known workarounds.

- CSCsa66305

With service policy applied to virtual template in the output direction, counters are incorrect.

There are no known workarounds.

- CSCsa67479

An interface configured as an E1 interface on the 24T1/E1 card will sometimes corrupt packets when placed in local loopback.

There are no known workarounds.

- CSCsa68004

A Service Selection Gateway (SSG) does not update tariff switch information to a user that logs in exactly at tariff switching time.

There are no known workarounds.

- CSCsa71157
 With 12.2(27.7.1)SIE7, a 7206VXR LAC stops responding whenever a single PPPoE session which needs to be forwarded to a LAC logs in.
 There are no known workarounds.
- CSCsa73382
 SSG is having a slow memory leak when host accounting is disabled.
 Workaround: Periodically reload the SSG to release memory
- CSCsa83649
 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.
- CSCsa85850
 You can configure more than the maximum bandwidth on ATM interfaces. This problem occurs in Cisco IOS Releases 12.3(9), 12.3(13b), and 12.3(11)T1.
 There are no known workarounds.
- CSCsb01157
 On a router with a large number of adjacencies, when multiple virtual-access interfaces are created the CPU load can get very high.
 There are no known workarounds.
- CSCsb02818
 If vpdn pre-cloning is configured on a Cisco 10000 series router, customer static routes may not be removed from the routing table after they disconnect.
 Workaround: Pre-cloning is not supported on the Cisco 10000 series router and should not be configured.
- CSCsb08566
 Repeatedly creating and removing AAA server groups may exhaust an internal table resource which causes further server group operations to fail. Some features such as SSG automatically create and remove AAA server groups and may trigger this problem.
 There are no known workarounds.
- CSCsb09312
 A Cisco router may stop responding by bus error when executing the command **sh idb** and wait for too long when the *more* prompt appears for sending the next page. The stop responding in itself being due to the idb not existing anymore at the time of printing the next page.
 Workaround: Set up term len 0 before issuing sh idb.
- CSCsb09928
 All traffic goes to class-default queue on ATM Virtual channels when the main ATM interface has an output policy-map applied. Output policy maps on the main ATM interface. The ATM VC is created (or comes up) after the policy-map is applied to the main ATM interface. This can happen due to either router reload or PRE switchover or configuration at different time.
 Workaround: Re-apply the service-policy on the main ATM interface.

- CSCsb14522
After router reload or PRE-switchover, no traffic is dequeued from the LLQ under the atm interface
router reload or PRE-switchover
Workaround: Remove and re-apply service policy from the interface
- CSCsb18973
SSG does not send attribute NAS-PORT[5] on the access request packet for a service with prepaid quota.
There are no known workarounds.
- CSCsb19966
After VBR-NRT VC is changed to UBR circuit, the SCR BW is not being released.
There are no known workarounds.
- CSCsb30553
Modifying queue-limit in a class when the policy-map is in use may cause the router to stop responding.
There are no known workarounds.
- CSCsb33599
RPR switchover from PRE-1 12.0(25)SX9 to PRE-2 12.2(27)SBB may take longer than expected, up to 30 minutes to have full traffic restoration This can also happen when 12.2S peers operate in RPR mode due to non-ISSU upgrade/downgrade or when upgrade to 12.2S from 12.3(7)XI
Workaround: This only occurs if the standby in RPR mode is running as standby for more than 35 minutes. To avoid the problem switch over before the standby is up that long or reset the standby, wait for it to come up again and then switch over within 35 minutes.
- CSCsb40055
A service name is absent from a service authorization request packet that is sent by an SSG to a prepaid server.
There are no known workarounds.
- CSCsb44002
When running multiple instances of the command **show PFX cpu queue ATM x/y/z** it is possible the Cisco 10000 series router may stop responding with a bus error.
There are no known workarounds.
- CSCsb47788
The output counters on a GE sub-if does not reflect the traffic traversing the interface. Both the SNMP ifOutOctets value and the CLI command **sh vlan dot1q gi 2/1/0.2** are incorrect.
There are no known workarounds.
- CSCsb50587
IP packets that are an odd number of bytes in length fail to be encapsulated in L2TP on a Cisco 10000 series router acting as LNS.
Workaround: Disable IP TOS reflect.

- CSCsb52703

Cisco 10000 series router is acting as a LNS. If PFC is not explicitly disabled with commands: **ppp pfc local forbid**, **ppp pfc remote reject** PFC is requested by LNS and in that case protocol field in outgoing ECHO replies is corrupted, i.e., it is 0xC0 instead of 0xC021.

Workaround: Use:
ppp pfc local forbid
ppp pfc remote reject

Note: With the workaround applied PFC will never be negotiated and can't be used in either direction.
- CSCsb57277

PXF causes the router to stop responding after we see the error message, Oct 7 16:30:44.777: %C10K_SESSION_GENERAL-3-EREVENT: Session-lookup: add_hw_session() no physical interface info for session :(16120)

Shut the VC's and clear sessions before modifying the VC's.
- CSCsb71982

PXF failed with DMA Toaster Fault error - Toaster IWRA Exception.

Workaround: Turn off Ingress Netflow; or prevent IP fragmentation; or upgrade to a release with the fix.
- CSCsb80624

Cisco 10000 series router reports a lot of error messages.

Workaround: Disable PXF queuing for the ATM interface with the command **no atm pxf queuing**.
- CSCsb83990

All the on-demand VC stuck on INAC state because not enough bandwidth error.

There are no known workarounds.
- CSCsb89005

A cisco10k running 12.3(7)X16 might reload as consequence of a software forced crash after a *c10k_tcm_write: Invalid Address* error

There are no known workarounds.
- CSCsb89096

Lawful intercept is designed to intercept the data packets through the router such as voice and data. This issue only happens when the customer setup a tap that it will intercept the packet to the router itself. In this case, an ICMP packet to the router.

There are no known workarounds.
- CSCsb89110

The system stops forwarding traffic with PPPoEoA using RADIUS option 242.

There are no known workarounds.
- CSCsb91807

Memory Utilization increases.

There are no known workarounds.

- CSCsc02602
The router stops responding when you detach service policy from QinQ subintf.
There are no known workarounds.
- CSCsc05532
Cisco 10008 PXF with PRE2 and 12.3(7)XI5 IOS experiences an alignment exception that results in the router stops responding.
There are no known workarounds.
- CSCsc12541
While issuing the **show interface pxf** command, a Cisco 10000 series router running 12.3(7)XI6 experiences high cpu usage and the console does not respond. The box is also not responding to ICMP packets.
Workaround: Do not issue the **show interface pxf** command.
- CSCsc14076
When you change an ATM PVC from VBR-NRT to UBR or the other way around, the subscribed bandwidth is incorrect, which is shown in the output of the **show controllers atm** command.
There are no known workarounds.
- CSCsc16798
On a Cisco 10000 router (Cisco 10008-PRE2) running 12.3(7)XI6 as LNS with mixed per-user ACL and access-group on the virtual-template, the access-lists could stop working as expected after some varying time.
Workaround: Avoid using per-user ACL mixed with access-groups.
- CSCsc19994
After the second switchover or ISSU upgrade, the 4-Port Channelized OC3 LC interfaces are down/down.
There are no known workarounds.
- CSCsc23981
Incorrect policing counters for per-user policy applied via RADIUS to VPDN customers. Affects VPDN but not PPPoE customers.
There are no known workarounds.
- CSCsc24427
On certain scenarios the toaster mtrie type 3 node will leak memory.
There are no known workarounds.
- CSCsc26489
Control traffic loss, PXF crash, this problem is seen once the Pak Priority queue created per interface is resized after drops are detected on the queue.
There are no known workarounds.
- CSCsc30938
On a Cisco 10000 series router, if either **show controllers atm slot/subslot/port fpga** or **show controllers atm slot/subslot/port> details** is entered on the console or through a telnet session, and through a separate telnet session, the router may stop responding.
There are no known workarounds.

- CSCsc37605
Traceback errors were observed after HA switchover cutover2.
There are no known workarounds.
- CSCsc39014
On a Cisco 10000 series router running 123-7.XI images the output for the command **show Facility-Alarm Status** will show alarms for T-1s that have never been configured. These T-1s will be outside the range that have ever been configured on the router.
There are no known workarounds.
- CSCsc40493
PPPoE sessions with long line-id tag cause PRE to stop responding.
There are no known workarounds.
- CSCsc42049
High CPU usage due to VTEMPLATE Background.
Workaround: Reload the router.
- CSCsc43860
PRE can stop responding when PPPoE pkt are received if vpdn and virtual template is missing and if a fiber cable is hooked up to a 4 Port OC3 line card.
Workaround: Have a fully working configuration.
- CSCsc44237
This caveat consists of two symptoms, two conditions, and two workarounds:
Symptom 1: A switch or router that is configured with a PA-A3 ATM port adapter may eventually run out of memory. The leak occurs when the FlexWAN or VIP that contains the PA-A3 port adapter is removed from the switch or router and not re-inserted.
The output of the **show processes memory** command shows that the "ATM PA Helper" process does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.
Workaround 1: Either do not remove the PA-A3 ATM port adapter from the FlexWAN or VIP or re-insert the PA-A3 ATM port adapter promptly. The memory leak stops immediately when the PA-A3 ATM port adapter is re-inserted.
Symptom 2: A switch or router that has certain PIM configurations may eventually run out of memory. The output of the **show processes memory** command shows that the "PIM process" does not have sufficient memory. The output of the **show memory allocating-process totals** command shows that the "Iterator" process holds the memory.
Workaround 2: When the **ip multicast-routing** command is configured, enable at least one interface for PIM. When the **ip multicast-routing vrf vrf-name** command is configured, enter the **ip vrf forwarding vrf-name** command on at least one interface that has PIM enabled.
- CSCsc49703
While PPPoE traffic is sent, VCs may not be created after Interfaces go down then up.
There are no known workarounds.
- CSCsc50308
Cisco 10000 series router stops responding due to a bus error.
There are no known workarounds.

- CSCsc53274
Memory corruption occurs on a Cisco 10000 series router, possibly leading to an unrequested reload.
Workaround: Do not configure standard ACLs on interfaces that are expected to do Lawful Intercept.
- CSCsc54609
RFC1483 packets received on an ATM VC configured for PPPoE will get forwarded without requiring a valid PPPoE session.
There are no known workarounds.
- CSCsc57332
Active PRE2 watchdog force reload -- c10k_pppox_inherit_given_queue.
There are no known workarounds.
- CSCsc60576
Cisco 10000 series router: Giga intf Input queue packets drop.
There are no known workarounds.
- CSCsc63858
Bus error crashes at **qos_set_mark_wrapper** command.
There are no known workarounds.
- CSCsc67238
A Cisco 10008 series router, PRE2 may stop responding with SSG configurations.
Workaround: Disable ssg service-overlap with the **no ssg service-overlap** command or avoid having overlapping networks in a service.
- CSCsc74916
Customer is seeing 4-Port Channelized STM/1 line card reloading multiple times.
There are no known workarounds.
- CSCsc83107
Packet counters for full VAIs are counted double. This problem seems to manifest when traffic originates from the Router Processor (RP) due to, for example, a ping. This is related to the fact that packets are then counted in the PXF as well as the RP.
There are no known workarounds.
- CSCsc89167
Inconsistency between IOS CEF and PXF CEF for a recursive route.
Workaround: Configure a static arp entry or, increase the timeout for the next hop or, ping from the RP to the next hop to resolve the issue.
- CSCsc89511
Interface flap with PPPoEoA on-demand VCs cause traceback.
There are no known workarounds.
- CSCsc91212
All T1's on 24-Port Channelized T1/E1 line cards are bouncing. **hw-mod reset** command recovers them.
There are no known workarounds.

- CSCsc91780
%SYS-3-CPUHOG in process DHCPD Timer.
There are no known workarounds.
- CSCsc96299
Punts to the RP due to a glean adjacency in the FIB can cause high RP CPU utilization.
There are no known workarounds.
- CSCsc96548
PRE may crash due to software forced crash after reporting %SYS-3-CPUHOG: process = STATS
DMA Daemon
There are no known workarounds.
- CSCsc99014
SSG miniACL that is converted to Turbo crashes the router Cisco 10000 Series Routers.
There are no known workarounds.
- CSCsd01816
Multilink Interface not recovering after flapping T-1 in bundle.
Workaround: Manually shut/no shut the affected multilink interfaces.
- CSCsd04745
All communications to the secondary PRE were lost until a hardware reset or reseating the card.
However, the error would return again shortly until the router was reloaded. Then, it would work fine for several hours until the error occurred again. This error was seen on both routers running XI7a crypto image in the test lab.
Workaround: DO NOT ISSUE **do show** command from inside a configuration prompt. Once this has been issued there is no workaround. A router reload is required to clear the error condition.
- CSCsd04873
Cisco 10000 Series Router interface resets.
There are no known workarounds.
- CSCsd15826
CPU goes to 100% usage, then RP stops responding.
There are no known workarounds.
- CSCsd27595
High CPU usage when shutting a main ATM interface with 8,000 + point-to-point subinterfaces underneath it.
Workaround: Configure fewer subinterfaces per main ATM interface. Use range VCs.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

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

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

**Tip**

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

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

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

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Copyright © 2006 Cisco Systems, Inc. All rights reserved.

