



Release Notes for the Cisco PDSN Feature in Cisco IOS Release 12.3(14)YX13

21 July 2008

Cisco IOS Release 12.3(14)YX13 is a special release that is based on Cisco IOS Release 12.3, with the addition of enhancements to the Cisco Packet Data Serving Node (Cisco PDSN) feature. The Cisco IOS Release 12.3(14)YX13 is a release optimized for the Cisco PDSN feature on the Cisco 7206VXR router, the Cisco 7609 Internet Router, the Cisco NPE-G1 router, and Cisco 6500 Catalyst Switch platform.

Contents

These release notes include important information and caveats for the Cisco PDSN software feature provided in Cisco IOS 12.3(14)YX13 for the Cisco 7206VXR series router, the Cisco 7609 Internet Router, and Cisco 6500 Catalyst Switch platforms.

Caveats for Cisco IOS Release 12.3 can be found on CCO at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/tsd_products_support_series_home.html

Release notes for Cisco 7000 Family for Release 12.3T can be found on CCO at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/prod_release_notes_list.html

Release notes for the Cisco 6000 Family for 12.3T can be found on CCO at:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/prod_release_notes_list.html

This release note includes the following topics:

- [Contents, page 1](#)
- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Upgrading to a New Software Release, page 4](#)
- [Packet Data Serving Node Software Features in Release 12.3\(14\)YX13, page 12](#)
- [Caveats, page 13](#)
- [Related Documentation, page 61](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Obtaining Documentation and Submitting a Service Request, page 66](#)

Introduction

Cisco PDSN is an IOS software feature that enables a Cisco 7206VXR router, or a Multi-Processor WAN Application Module (MWAM) on a Catalyst 6500 Switch or 7600 Internet router, or the Cisco NPE-G1 router to function as a gateway between the wireless Radio Access Network (RAN) and the Internet. With Cisco PDSN enabled on a router, a stationary or roaming mobile user can access the Internet, a corporate network intranet, or Wireless Application Protocol (WAP) services. Cisco PDSN supports both Simple IP operation and Mobile IP operation.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(14)YX13:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 3](#)
- [Software Compatibility, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 4](#)
- [MIBs, page 11](#)

Memory Requirements

[Table 1](#) shows the memory requirements for the PDSN Software Feature Set that supports the Cisco 7206VXR router, the MWAM card on the Cisco 6500 Catalyst Switch platform and 7600 Internet router platform, and the Cisco NPE-G1 router. The table also lists the memory requirements for the IP Standard Feature Set (for the Home Agent [HA]).

Table 1 *Memory Requirements for the Cisco 7206VXR Router and MWAM on the 6500 Catalyst Switch and 7600 Router*

Platform	Software Feature Set	Image Name	Flash Memory Required	DRAM Memory Required	Runs From
Cisco 7206VXR Router	PDSN Software Feature Set	c7200-c6is-mz.123-14.YX13 c7200-c6ik9s-mz.123-14.YX13	20 MB	512 MB	RAM
Cisco 6500 Catalyst Switch	PDSN Software Feature Set	c6svc5fmwam-c6is-mz (This is a bundled image)	40MB	512MB	RAM
Cisco 7600 Internet Router	PDSN Software Feature Set	c6svc5fmwam-c6is-mz (This is a bundled image)	40MB	512MB	RAM
Cisco NPE-G1 Router	PDSN Software Feature Set	c7200-c6is-mz.123-14.YX13 c7200-c6ik9s-mz.123-14.YX13	40MB	512MB	RAM

Hardware Supported

Cisco IOS Release 12.3(14)YX13 is optimized for the Cisco PDSN feature on the Cisco 7206VXR router, the MWAM card on the Cisco 6500 Catalyst Switch platform and 7600 Internet router platform, and the Cisco NPE-G1 router.

A Hardware-Software Compatibility Matrix is available on CCO for users with CCO login accounts. This matrix allows users to search for supported hardware components by entering a Cisco platform and IOS Release. The Hardware-Software Compatibility Matrix tool is available at the following URL:

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswwmatrix.cgi>

Software Compatibility

Cisco IOS Release 12.3(14)YX13 is a special release that is developed on Cisco IOS Release 12.3.

Cisco IOS Release 12.3(14)YX13 supports the same features that are in Cisco IOS Release 12.3, with the addition of the Cisco PDSN feature.

Determining the Software Version

To determine the version of Cisco IOS software running on your router, log in to the router and enter the **show version EXEC** command:

```
Router#show version
Router#sh ver
Cisco IOS Software, MWAM Software (MWAM-C6IS-M), Version 12.3(14)YX, RELEASE SOFTWARE
(fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2005 by Cisco
Systems, Inc.
Compiled Mon 25-Jul-05 15:24 by ssearch

ROM: System Bootstrap, Version 12.2(11)YS2 RELEASE SOFTWARE

Router uptime is 2 hours, 9 minutes System returned to ROM by reload at 07:35:31 UTC Wed
Jul 6 2005 System restarted at 02:31:05 UTC Tue Jul 26 2005 System image file is
"svcmwam-c6is-mz"

Cisco MWAM (MWAM) processor with 473088K/32768K bytes of memory.
SB-1 CPU at 700MHz, Implementation 1025, Rev 0.2

Last reset from power-on
1 Gigabit Ethernet interface
511K bytes of non-volatile configuration memory.

Configuration register is 0x4

Router#
```

Upgrading to a New Software Release

The following sections contain details on how to upgrade your Cisco Mobile Wireless Home Agent:

- [Upgrading PDSN Image from YF-based Image to 12.3\(14\)YX Image](#)
- [Upgrading the Supervisor Image](#)
- [Upgrading the PDSN Image on MWAM](#)
- [Upgrading the Member PDSN on MWAM](#)
- [Changing Configuration on the PDSN in a Live Network](#)

Upgrading PDSN Image from YF-based Image to 12.3(14)YX Image

If you are upgrading the PDSN from a YF-based image to a 12.3(14)YX image, you first need to upgrade the SUP image from a SXB-based image to the recommended SXE-based image.



Note

We recommend that you upgrade to the Cisco IOS Supervisor Engine 720, Release 12.2(18)SXE3.

For more information on the 12.2(18)SXE3 Supervisor image, please refer to the following URL: http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html

After you upgrade the SUP image, you can then upgrade the PDSN image.

Upgrading the Supervisor Image

To upgrade the Supervisor image, perform the following procedure:

-
- Step 1** Copy the SUP image to the disks (disk0: / slavedisk0:).
- Step 2** Add the following command to the running config boot system disk0: *SUP image name*. Here is an example:

```
boot system disk0:s72033-advipservicesk9_wan-mz.122-18.SXE3.bin
```



Note

This step may require you to unconfigure previously configured instances of this CLI in order to enable the image to properly reload.

- Step 3** Perform a “write memory” so that running configuration is saved on both active and standby SUP.
- Step 4** Issue **reload** command on the active SUP.

Both active and standby SUP will reload simultaneously and come up with the SXE3-based image.



Note

Issuing the **reload** command on the active SUP will cause both the active and standby Supervisors to reload simultaneously, thus causing some downtime during the upgrade process.

Upgrading the PDSN Image on MWAM

To upgrade an image on the Cisco MWAM, you will need a compact flash card that has the MP partition from the current image or later, and a recent supervisor image. To locate the images, please go to the Software Center at Cisco.com (<http://www.cisco.com/public/sw-center/>)

Upgrading the Controller PDSN on MWAM:

To upgrade to an IOS 12.3(14)YX image on the PDSN controller, perform the following procedure:

- Step 1** Bring down the Standby PDSN Controller Loaded with YF based image, by issuing the **hw-module module slot # reset cf:1** command on Supervisor. The active PDSN Controller will continue to service the incoming requests.

Log onto the supervisor and boot the MP partition on the PC.

```
SUP-PDSN#hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]
% reset issued for module 8
SUP-HA#
SUP-HA#
Nov 10 18:01:29.624: %SNMP-5-MODULETRAP: Module 8 [Down] Trap
Nov 10 18:01:29.624: SP: The PC in slot 8 is shutting down. Please wait ...
Nov 10 18:01:55.252: SP: PC shutdown completed for module 8
Nov 10 18:01:55.256: %C6KPWR-SP-4-DISABLED: power to module in slot 8 set off (Reset)
Nov 10 18:04:00.195: SP: OS_BOOT_STATUS(8) MP OS Boot Status: finished booting
Nov 10 18:04:42.299: %SNMP-5-MODULETRAP: Module 8 [Up] Trap
Nov 10 18:04:42.271: %DIAG-SP-6-BYPASS: Module 8: Diagnostics is passed
Nov 10 18:04:43.143: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
SUP-PDSN#
```

- Step 2** Once the module is online, copy the 12.3(14)YX image to pclk# slot file system by issuing the following command:

copy tftp: tftp file location pclk# linecard #-fs:

The upgrade file uses a special format that makes this process slow. The following example illustrates the upgrade process output:

```
SUP-PDSN#$/10.77.155.10/pdsn/images/c6svc5fmwam-hlis-mz.R30_11092005 pclk#8-fs:
Destination filename [c6svc5fmwam-hlis-mz.R30_11092005]?
Accessing tftp://10.77.155.10/pdsn/images/c6svc5fmwam-hlis-mz.R30_11092005...
Loading pdsn/images/c6svc5fmwam-hlis-mz.R30_11092005 from 10.77.155.10 (via Vlan10):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
[OK - 24168088 bytes]
```

```

24168088 bytes copied in 192.376 secs (125629 bytes/sec)
SUP-PDSN#
Nov 10 18:09:03.903: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has started>
Nov 10 18:09:03.903: %SVCLC-SP-5-STRRECVD: mod 8: <Do not reset the module till upgrade
completes!!>
Nov 10 18:09:42.022: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has succeeded>
Nov 10 18:09:42.022: %SVCLC-SP-5-STRRECVD: mod 8: <You can now reset the module>
SUP-PDSN#

```

- Step 3** Now boot the MWAM card back to partition 4, the processor comes back as standby unit, and you have an upgraded image on standby PDSN controller.

```

SUP-PDSN#hw-module module 8 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]
% reset issued for module 8
SUP-PDSN#
Nov 10 18:10:34.831: %SNMP-5-MODULETRAP: Module 8 [Down] Trap
Nov 10 18:10:34.831: SP: The PC in slot 8 is shutting down. Please wait ...
Nov 10 18:10:57.387: SP: PC shutdown completed for module 8
Nov 10 18:10:57.391: %C6KPWR-SP-4-DISABLED: power to module in slot 8 set off (Reset)
Nov 10 18:12:13.370: SP: OS_BOOT_STATUS(8) MWAM
Nov 10 18:14:30.447: %SNMP-5-MODULETRAP: Module 8 [Up] Trap
Nov 10 18:14:30.434: %DIAG-SP-6-BYPASS: Module 8: Diagnostics is passed
Nov 10 18:14:31.293: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online

```

- Step 4** Verify that all the bindings serviced by the active PDSN controller running the YF image have been synched with the newly brought up standby PDSN controller running the 12.3(14)YX PDSN image. The same can be verified by issuing the following show command on Active and Standby PDSN controller.

```

7600a-cont2# show cdma pdsn cluster controller member load

```

Secs until (past) seek	Seq seeks no reply	Member IPv4 Addr	State	Load	Sessions
2	0	20.20.10.2	ready	0	15
8	0	20.20.10.1	ready	0	15

```

-----
Controller IPv4 Addr 20.20.101.105

```

```

7600a-cont2# show cdma pdsn cluster controller session count
30 session records

```

- Step 5** Bring down the active PDSN Controller with the YF-based image. The newly upgraded standby PDSN controller (running 12.3(14)YX PDSN image) becomes the active unit.
- Step 6** Perform steps 1 through 3 as described above.
- Step 7** Verify that all the bindings serviced using the active PDSN controller running the 12.3(14)YX image have been synched with the newly enabled standby PDSN controller running the 12.3(14)YX PDSN image. The same can be verified by issuing the following show command on active and standby PDSN controller.

```
7600a-cont1#show cdma pdsn cluster controller member load
```

Secs until (past) seek	Seq seeks no reply	Member IPv4 Addr	State	Load	Sessions
2	0	20.20.10.2	ready	0	15
8	0	20.20.10.1	ready	0	15

Controller IPv4 Addr 20.20.101.105

```
7600a-cont1# show cdma pdsn cluster controller session count
30 session records
```



Note We recommend that you remove the “HSRP Preemption” configuration between the active and standby PDSN Controller before proceeding with the Upgrade/Downgrade Procedure.



Note The downgrade process is similar to the upgrade process, where the SUP image should be downgraded first, followed by the PDSN image.



Note If config-on-SUP mode (mwam config-mode supervisor) is used on MWAM, the startup configuration is written on the SUP. This will assist you in upgrading/downgrading the images without losing the PDSN configuration between the YF and 12.3(14)YX images.

Upgrading the Member PDSN on MWAM

To upgrade to the 12.3(14)YX image on the PDSN, perform the following procedure:

- Step 1** In PDSN cluster environment you can segregate a member PDSN out of the cluster by configuring the following command on the member PDSN, so that no new request from mobile node are entertained by this member:

```
7600a-pdsn1(config)# cdma pdsn cluster member prohibit administratively
```

The calls, which are already connected to the member, will be alive until the mobile node disconnects the call. Alternatively, the calls can be forcibly cleared on the prohibited member using the following command:

```
7600a-pdsn1(config)# clear cdma pdsn session all
```

- Step 2** Now bring down the PDSN Loaded with YF based image, by issuing the **hw-module module slot # reset cf:1** command on Supervisor.

Log onto the supervisor and boot the MP partition on the PC.

```
SUP-PDSN# hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.
```

```
Proceed with reload of module?[confirm]
% reset issued for module 8
SUP-HA#
```

```

SUP-HA#
Nov 10 18:01:29.624: %SNMP-5-MODULETRAP: Module 8 [Down] Trap
Nov 10 18:01:29.624: SP: The PC in slot 8 is shutting down. Please wait ...
Nov 10 18:01:55.252: SP: PC shutdown completed for module 8
Nov 10 18:01:55.256: %C6KPWR-SP-4-DISABLED: power to module in slot 8 set off (Reset)
Nov 10 18:04:00.195: SP: OS_BOOT_STATUS(8) MP OS Boot Status: finished booting
Nov 10 18:04:42.299: %SNMP-5-MODULETRAP: Module 8 [Up] Trap
Nov 10 18:04:42.271: %DIAG-SP-6-BYPASS: Module 8: Diagnostics is passed
Nov 10 18:04:43.143: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
SUP-PDSN#
    
```

Step 3 Once the module is online, copy the 12.3(14)YX image to pclk# slot file system by issuing the following command:

```
copy tftp: tftp file location pclk# linecard #-fs:
```

The upgrade file uses a special format that makes this process slow. The following example illustrates the upgrade process output:

```

SUP-PDSN#$/10.77.155.10/pdsn/images/c6svc5fmwam-hlis-mz.R30_11092005 pclk#8-fs:
Destination filename [c6svc5fmwam-hlis-mz.R30_11092005]?
Accessing tftp://10.77.155.10/pdsn/images/c6svc5fmwam-hlis-mz.R30_11092005...
Loading pdsn/images/c6svc5fmwam-hlis-mz.R30_11092005 from 10.77.155.10 (via Vlan10):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
[OK - 24168088 bytes]

24168088 bytes copied in 192.376 secs (125629 bytes/sec)
SUP-PDSN#
Nov 10 18:09:03.903: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has started>
Nov 10 18:09:03.903: %SVCLC-SP-5-STRRECVD: mod 8: <Do not reset the module till upgrade
completes!!>
Nov 10 18:09:42.022: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has succeeded>
Nov 10 18:09:42.022: %SVCLC-SP-5-STRRECVD: mod 8: <You can now reset the module>
SUP-PDSN#
    
```

Step 4 Now boot the MWAM card back to partition 4, the processor comes back online, and you have an upgraded image on PDSN.

```

SUP-PDSN#hw-module module 8 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]
% reset issued for module 8
SUP-PDSN#
Nov 10 18:10:34.831: %SNMP-5-MODULETRAP: Module 8 [Down] Trap
Nov 10 18:10:34.831: SP: The PC in slot 8 is shutting down. Please wait ...
Nov 10 18:10:57.387: SP: PC shutdown completed for module 8
Nov 10 18:10:57.391: %C6KPWR-SP-4-DISABLED: power to module in slot 8 set off (Reset)
Nov 10 18:12:13.370: SP: OS_BOOT_STATUS(8) MWAM
Nov 10 18:14:30.447: %SNMP-5-MODULETRAP: Module 8 [Up] Trap
    
```

```
Nov 10 18:14:30.434: %DIAG-SP-6-BYPASS: Module 8: Diagnostics is passed
Nov 10 18:14:31.293: %OIR-SP-6-INSCARD: Card inserted in slot 8, interfaces are now online
```

- Step 5** Join the member PDSN with the cluster environment by configuring the following command on the member PDSN, so that the controller can direct new incoming request to this member PDSN as well.

```
7600a-pdsn1(config)# no cdma pdsn cluster member prohibit administratively
```



Note The downgrade process is similar to the upgrade process, where the SUP image should be downgraded first followed by the PDSN image. Additionally, ensure all session redundancy specific configuration on PDSN was removed before downgrading to the YF-based image.



Note If config-on-SUP mode (mwam config-mode supervisor) is used on MWAM, the startup configuration is written on SUP. This will assist you in upgrading/downgrading the images without losing the PDSN configuration between YF and 12.3(14)YX images.

Changing Configuration on the PDSN in a Live Network

If you need to change the working configuration on a PDSN in a live network environment, perform the following procedure:

- Step 1** Bring the standby PDSN out of service. An example would be to unconfigure the **cdma pdsn redundancy** command on the standby PDSN. This isolates the standby PDSN from the session redundancy setup.
- Step 2** Perform a “write memory” so that running configuration is saved.
- Step 3** Now make the necessary configuration changes on the standby PDSN, and save the configuration.
- Step 4** Re-configure the **cdma pdsn redundancy** command, and save the configuration.
- Step 5** Issue the **reload** command to bring the standby PDSN back into the session redundancy setup with the changed configuration. Verify the processor comes back in the SR setup using the following show commands:

```
7600a-Stdy#show standby brief
                P indicates configured to preempt.
                |
Interface  Grp Prio P State   Active           Standby           Virtual IP
Gi0/0.101  300 110   Standby 20.20.101.10    local             20.20.101.101

7600a-Stdy# show cdma pdsn redundancy
CDMA PDSN Redundancy is enabled

CDMA PDSN Session Redundancy system status
PDSN state = STANDBY HOT
PDSN-peer state = ACTIVE

CDMA PDSN Session Redundancy Statistics
Last clearing of cumulative counters never
                Total           Current
                Synced from active   Connected
Sessions                15                 15
```

```

SIP Flows          15          15
MIP Flows          0           0
PMIP Flows         0           0

```

```

7600a-Stdy#show redundancy inter-device
Redundancy inter-device state: RF_INTERDEV_STATE_STDBY
Scheme: Standby
  Groupname: pdsn-rp-sr1 Group State: Standby
Peer present: RF_INTERDEV_PEER_COMM
Security: Not configured

```

```

7600a-Stdy#show redundancy states
my state = 8 -STANDBY HOT
peer state = 13 -ACTIVE
  Mode = Duplex
  Unit ID = 0

  Split Mode = Disabled
  Manual Swact = Enabled
  Communications = Up

  client count = 9
  client_notification_TMR = 30000 milliseconds
  RF debug mask = 0x0

```

```
7600a-Stdy#
```

Step 6 Now make the standby PDSN to takeover as active by reloading the current active PDSN.



Note Some outage might occur while performing this step concerning existing calls on the active PDSN (which is being taken out of service), when synched with newly active unit because of change in configuration.

Step 7 Perform Step 1 to Step 5 on current standby PDSN.



Note Configurations on the active and standby should be the same for PDSN SR to work properly.



Note We recommend that you disable the “HSRP preemption” configuration on the active and standby PDSN before proceeding with the configuration changes.

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Upgrade Ordering Instructions* located at:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in [Table 2](#).

Table 2 *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be decided
OLD-CISCO-DECNET-MIB	To be decided
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be decided
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be decided
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be decided

Cisco IOS Feature Sets

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.3(14)YX13 supports the same feature sets as Cisco Release 12.3, with the exception that Cisco Release 12.3(14)YX13 includes the PDSN feature. The PDSN feature is optimized for the Cisco 7206VXR router, the Cisco MWAM card on the 6500 Catalyst Switch and 7600 Internet router, and the Cisco NPE-G1 router.



Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Packet Data Serving Node Software Features in Release 12.3(14)YX13

The Cisco IOS Release 12.3(14)YX13 supports the same feature sets as Cisco Release 12.3, with the exception that Cisco Release 12.3(14)YX13 includes the PDSN feature. The Cisco PDSN feature is optimized for the Cisco 7206VXR router, the Cisco MWAM card on the 6500 Catalyst Switch and 7600 Internet Router, and the Cisco NPE-G1 router, and includes the following features:

- Support for Mobile Equipment Identifier (MEID)
- Simple IPv6 Access
- Session Redundancy Infrastructure
- Radius Server Load Balancing
- Closed-RP/Open-RP Integration
- Subscriber Authorization Based on Domain
- PDSN MIB Enhancement
- PPP Counters
- RP Counters
- Conditional Debugging Enhancements
- Trace Functionality
- Mobile IP Dynamic Home Address Deletes Older Sessions With Different IMSI
- Protocol Layering and RP Connections
- PPPoGRE RP Interface
- A11 Session Update
- SDB Indicator Marking
- Resource Revocation for Mobile IP
- Packet of Disconnect
- IS-835 Prepaid Support
- Prepaid Billing
- Mobile IP Call Processing Per Second Improvements
- IS-835-B Compliant Static IPsec
- Always On Feature
- NPE-G1 Platform Support
- PDSN Cluster Controller / Member Architecture
- PDSN MIB Enhancement
- Conditional Debugging Enhancements
- PDSN Cluster Controller / Member Architecture
- PDSN MIB Enhancement
- Cisco Proprietary Prepaid Billing
- 3 DES Encryption

- Mobile IP IPSec
- Hardware IPSec Acceleration Using IPSec Acceleration Module—Static IPSec
- 1xEV-DO Support
- Integrated Foreign Agent (FA)
- AAA Support
- Packet Transport for VPDN
- Proxy Mobile IP
- Multiple Mobile IP Flows

All other software features in Cisco IOS Release 12.3 are described in the documentation for Cisco IOS Release 12.3, which can be found at:

http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

Caveats for Cisco IOS Releases 12.3 can be found on CCO at http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_release_notes_list.html

The “[Open Caveats](#)” section lists open caveats that apply to the current release and might also apply to previous releases.

The “[Resolved Caveats](#)” section lists caveats resolved in a particular release, which may have been open in previous releases.



Note

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco Bug Toolkit: Cisco Bugtool Navigator II**, or at <http://www.cisco.com/support/bugtools>.

Open Caveats

The following caveats are unresolved in Cisco IOS Release 12.3(14)YX12:

- CSCso89250—Gigaword Attributes Not Sent During IS835b Handoff
Acct-Input-Gigawords and Acct-Output-Gigawords are not sent during handoff.
This condition occurs when the handoff performed is is-835b.
Workaround: perform is-835a handoff by configuring the **cdma pdsn compliance is835a handoff** command.
- CSCsq00293—MWAM Image Upgrade Issue When Using SRC Image in Sup.
On a Cisco router running Release 3.0 PDSN software, there is an MWAM image upgrade issue on using SRC Image in sup .
This issue is seen in the Cisco IOS 12.3(14)YX12 image.
Workaround: none.

Unresolved Caveats Prior to 12.3(14)YX12

There are no new unresolved caveats in Cisco IOS Release 12.3(14)YX11.

Unresolved Caveats Prior to 12.3(14)YX11

There are no new unresolved caveats in Cisco IOS Release 12.3(14)YX10.

Unresolved Caveats Prior to 12.3(14)YX10

The following caveats are unresolved in Cisco IOS Release 12.3(14)YX8:

CSCsi53373—PDSN Reloads on Switch From HDLCoGRE to PPPoGRE

On a Cisco router running the Release 3.0 PDSN YX6 software, a reload occurs when a HDLCoGRE protocol type session is moved to dormant, and a dormant handoff is made to a PCF with a PPPoGRE protocol type. The reload occurs when the session is brought back to active in the current PCF and moved to dormant.

Workaround: none.

Unresolved Caveats Prior to 12.3(14)YX8

The following caveats are unresolved in Cisco IOS Release 12.3(14)YX4:

CSCsg25818—Acct-Session-Time Attribute Being Sent with Wrong Value

On a Cisco router running Cisco IOS 12.3(14)YX4 software, when a dormant handoff is done and the session is closed down, the acct-session-time is sent with a wrong value. This issue occurs only in a Session Redundancy (SR) setup when doing double switch over from the active to standby, and back to active.

Workaround: none.

- CSCse32483—Bus error at ip_fastswitch.

On a Cisco router running Cisco IOS 12.3(14)YX software, the PDSN may experience a bus error or a stack low warning message for a Level 1 interrupt. This occurs when there is heavy mobile to mobile traffic, with both the sender and receiver mobiles connected to the same PDSN. This does not happen on regular uplink or downlink traffic (traffic to outside network).

Workaround: none.

- CSCsg33992—Memleak Seen During PPP Renego Using Sub Interfaces

On a Cisco router running the Cisco IOS 12.3(14)YX software, a memory leak of 64 bytes per session occurs in all PPP renegotiations initiated by the MN or the PDSN. This occurs on all PDSN images with sessions created using sub interfaces (virtual-access sub interfaces).



Note

In YF images, the TCP header compression created full interfaces, but in YX only sub interfaces are created.

Workaround: configure the **ip irdp** command on the Virtual-Template.

Here is a sample configuration:

```
interface Virtual-Template1
 ip unnumbered Loopback0
```

```

ip mobile foreign-service challenge
ip mobile foreign-service reverse-tunnel
ip irdp<--- Needed as a workaround
no ip route-cache
no logging event link-status
peer default ip address pool pdsn-pool
peer default ipv6 pool PDSN-Ipv6-Pool
no keepalive
ppp accm 0
ppp authentication pap chap optional
ppp accounting none

```

Unresolved Caveats Prior to 12.3(14)YX4

The following caveats are unresolved in Cisco IOS Release 12.3(14)YX3:

- **CSCse29358**—Service-Option (F5) is Set to 0 in Acct-Stop During Handoff.

On a Cisco router running 12.4(7.9.1) PIL5 software, the Service-Option value set to **0** in Acct-Stop message during dormant / Active handoff.

Workaround: none.
- **CSCse39034**—IO mEmory Depletion With Slow RADIUS Server Responses

An MWAM card running version 2.1 of the PDSN software can experience low IOMEM conditions. When this occurs, it may not be possible to session to the processor consoles. Tracebacks relating to IO Memory allocation failure may also be seen.

This condition occurs when the load on the RADIUS server used for authentication and accounting is high and there are a large number of RADIUS timeouts and subsequent re-transmissions.

Workaround: ensure that the number of RADIUS timeouts and re-transmissions is not excessive.
- **CSCse63330**—MWAM/PDSN -MIP RRP Does Not Contain New Challenge For Re-registration

When using the simulator image to generate MIP call to the PDSN R2.1 12.3(11)YF3, PDSN does not send a new MN-FA challenge in RRP for MN to use on its next attempt at re-registration.

In situations where the previous RRQ failed due to code 136 (unknown HA address), RRP does not contain any challenge extension (let alone new extension for next registration). This behavior results in a “stale challenge error condition” where the re-registration continuously uses the first challenge extension that produced error code 136.

Workaround: none.
- **CSCse71921**—Release Indicator Not Sent While Doing Active-Handoff After Switchover

On a Cisco router running 12.3(14)YX3 software, the F13 Release Indicator is not sent in an Accounting Stop message for the old PCF, while doing active-handoff after switchover.

Workaround: none.
- **CSCse71950**—PDSN is reusing the same C1 (Account Session ID) value sent in an acct-start at the time of session opening, and in the start-stop pair for new pcf at dormant handoff time.

On a Cisco router running 12.3(14)YX3 software, the PDSN reuses the same C1 (Account Session ID) value sent in acct-start at the time of session opening, and in the start-stop pair for new pcf at dormant handoff time.

Workaround: none.

- CSCse71974—Multiple Acct Msgs Sent When Airlink Active Start Message Received.

For non-sr cases, after doing a dormant handoff, when an airlink active start message is received, the PDSN is sending 3 accounting packets instead of a single accounting packet.

On Cisco router running 12.3(14)YX3 software, after doing dormant handoff, if we send an airlink active start, PDSN is sending three accounting packets instead of single accounting start packet.

Workaround: none.

- CSCse72317—Duplicate Correlation Ids From PDSN

On Cisco router running the PDSN image, duplicate correlation IDs are seen.

This condition occurs when a user (NAI) connects with different MN identities (IMSI/MIN) using different HAs.

In this scenario for an already existing MN session, if the same user (same NAI in Mobile IP RRQ) connects with a different MN identity and HA address, the correlation ID for the session is reused.

Workaround: none.

Unresolved Caveats Prior to 12.3(14)YX3

The following caveats are unresolved in Cisco IOS Release 12.3(14)YX2:

- CSCsd46212—SNMP Query Does Not Return Any Value for cCdmaHDLCoGRESessionTotal

The SNMP get for the MIB object cCdmaHDLCoGRESessionTotal is not returning any value. getmany on cCdmaHDLCoGRESessionTotal returns nothing.

Workaround: none.

- CSCse09464—Standby Cluster Controller Reloaded When Unconfiguring Controller I/F

On a Cisco router running 12.3(14)YX1 PDSN software, the standby cluster controller reloaded when unconfiguring the controller interface, this is not seen consistently.

Workaround: none.

- CSCse14819—SNMP Query on cmiFaAdvertChallengeValue Falls Into Infinite Loop

SNMP walk on MIB variable cmiFaAdvertChallengeValue (OID: .1.3.6.1.4.1.9.9.174.1.1.2.2.1.2), the query falls into an infinite loop.

Workaround: none.

Unresolved Caveats Prior to 12.3(14)YX2

The following caveats are unresolved in Cisco IOS Release 12.3(14)YX1:

- CSCsd01351—First Start Airlink Record Received After Setup is Not Synced to Standby
The first start airlink record received after setup is not synced to the standby.
Workaround: there is no workaround. Since the setup airlink record is synced to the standby, sending the attributes in the setup airlink record could be a possible workaround.
- CSCsd70914—PPP Termination Counter Does Not Get Incremented After Session Timeout
On a Cisco router the Cisco IOS Release 12.3(14)YX1 image, when a Closed-RP simple-ip session gets closed due to session timeout, the PPP Termination Counter under the RP statistics does not get incremented.
This condition occurs on a PDSN configuration using the IOS 12.3(14)YX1 image.
Workaround: none.
- CSCsd78129: PSDN Memory Leak at PPP Related Process
On a Cisco router running version 2.1 of the PDSN software, the memory held by the PPP Events and PPP Hooks processes may increase continuously.
This condition occurs when PPP sessions are being opened and closed.
Workaround: none.
- CSCsd79413—PDSN Bus Error
The PDSN reloads due to a bus error.
This condition occurs on a MWAM running the 12.3(11)YF4 software. The PDSN reloads after a packet pool corruption error message is logged on to the console. This is observed in the following scenario:
 - PDSN is usually managing around 6000 PPP sessions
 - The aggregated traffic amounts to 60-70 Mbps
 - There are between 20-30 RADIUS accounting events per seconds
 - The CPU load is around 50%**Workaround:** none.
- CSCsd84703—**ip mobile cdma** CLI Chain Broken
On a Cisco router running the 12.3(14)YX1 software, the **ip mobile cdma** command chain was broken.
Workaround: none.

Unresolved Caveats Prior to Cisco IOS 12.3(14)YX1

The following caveats are unresolved in Cisco IOS Release 12.3(14)YX:

- CSCin95659—AAA debugs are Not Prepended With Username When Conditional Debugging Is Enabled.
On a Cisco PDSN running the Cisco IOS 12.3(14) YX PDSN Image, AAA debugs are not prefixed with username when conditional debugging for the username is enabled.
Workaround: none.

- CSCin97998—PPP Connection Request Does Not Match With Success + Failure + Aborted
On a Cisco PDSN running the Cisco IOS 12.3(14) YX PDSN Image, the PPP connection success is not getting incremented after the connection comes up.
This happens only when IPv6 session is opened.
Workaround: disable cdma ipv6 support.
- CSCin98027—PDSN Not Negotiating Interface-Id in IPv6CP in Passive Mode
On a Cisco PDSN running the Cisco IOS 12.3(14) YX PDSN Image, the Interface-ID is not being negotiated during ipv6cp negotiation by PDSN when PDSN is configured under passive mode.
This happens when the PDSN is configured in passive mode.
Workaround: configure the PDSN in active mode.
- CSCsb69576—Standby ODAP Client Allocating Address When Framed IP address is Used
On a Cisco router running PDSN Software, when framed IP address is configured in AAA for a user and a session is opened, the standby ODAP client allocates address from its leased subnet.
This occurs only when Framed IP address is used from AAA and ODAP is configured for address allocation.
Workaround: none.
- CSCsb84585—Issues with Trace Functionality for Mobile IP Debugs
On a Cisco PDSN running the Cisco IOS 12.3(14)YX PDSN Image, the following issues occur:
 - a. While testing conditional debugging triggered with IMSI for Mobile-IP debugs, a few of the debugs do not get prepended with IMSI value.
 - b. By configuring **ip mobile debug include username**, all the debugs get prepended with **Username** even without enabling **conditional debugs**.**Workaround:** none.
- CSCsb97395—Rare Traceback on PDSN Due to Word Alignment While Opening PMIP Flow
On a Cisco PDSN running the Cisco IOS 12.3(14)YX PDSN Image, traceback is seen on PDSN while opening the PMIP flow due to improper word alignment.
This is not continuously reproducible.
Workaround: none.
- CSCsc42997—Missing username info for some conditional debugs during ipcp/ccp nego
On a Cisco PDSN running the Cisco IOS 12.3(14)YX PDSN Image, ipcp and ccp negotiations under ppp are not prepended with username when conditional debugging is enabled.
Workaround: none.
- CSCsc43200—Tracebacks in Members of 8-member Cluster During Standby-Active Transition
On a Cisco router running Packet Data Serving Node(PDSN), tracebacks are occasionally seen on the members of a 8-member SR cluster when a PDSN transitions from the standby to the active state with SIP and MIP sessions being flapped at 500 and 350 CPS respectively.
Workaround: none.

- CSCsc46228—SIPv6: PDSN Session Counters Incorrect

On Cisco router running Packet Data Serving Node(PDSN), the following issues are seen with the session and accounting counters when **cdma pdsn ipv6** is configured:

- ipv6 packets are not counted in Acct-Input-Packets and Acct-Output-Packets, in accounting messages.
- ipv6 packets are counted in Acct-Input-Octets and Acct-Input-Packets, but do not reset after the session become dormant (accounting stop is sent out).
- In case of ipv4, ipv6 sharing a flow, ipv4 counters in **show cdma pdsn session** displays traffic count for both ipv4 and ipv6.
- In case of **ipv6 cef** enabled on the router, Acct-Input-Octets and Acct-Input-Packets are not counted for ipv6 traffic and also are not displayed in **show cdma pdsn session**.

Workaround: none.

- CSCsc46303—MIB Sanity Check RP Update and ACK Counters Does Not Match

On a Cisco PDSN running the Cisco IOS 12.3(14)YX PDSN Image, “CdmaRpUpdTransmittedReqs” counter values does not match with the sum of “CdmaRpUpdateAccepted”, “CdmaRpUpdateDenied” and “CdmaRpUpdateNotAked” counters. This issue is seen only in a rare scenario.

Workaround: none.

- CSCsc66758—SIPv6 Session Brought Down Due to IPCP Failure

On a Cisco router running Packet Data Serving Node (PDSN) with **cdma pdsn ipv6** and **IPv6 cef** enabled, when a dual stack MN tries to bring up IPCP and IPv6CP, if the IPv4 address allocation fails due to any reason, the PDSN tears down the IPv6 flow too, for the MN.

This behavior is not seen consistently

Workaround: none.

- CSCsc69520—F13 Not Sent in Accounting Stop Record When a Dormant Session Tears Down

On Cisco router running 12.3(14)YX PDSN software, the F13 attribute not sent in accounting stop, when a dormant session is torn down.

This issue is seen only when the session is closed during dormant state.

If the session is torn down while it is in active state, then no issues seen.

Workaround: none.

- CSCsc74745—PDSN Deletes Old PCF Details When Ppp Negotiation Starts During Handoff

On a Cisco router running PDSN IOS release 12.3(11)YF software, if the PPP re-negotiation starts for the mobile during the handoff, the PDSN deletes the Old PCF details.

Workaround: enable the following command on the PDSN: **cdma pdsn compliance is835a handoff**.

- CSCsc77152—RRQ Re-transmitted Before Timeout and with Different HA Address for PMI

On Cisco router running 12.3(14)YX PDSN software, RRQs are being re-transmitted before retransmit timeout and with different HA address for PMIP flow with HA-SLB. Also there is no command to configure re-transmit value for RRQ incase of PMIP flow.

Workaround: None

- CSCsc66482—SipV6: Ingress Address Filtering not Working With **ipv6 cef** Enabled
On Cisco router running 12.3(14)YX Packet Data Serving Node (PDSN) with **cdma pdsn ipv6** and **ipv6 cef** enabled, the ingress address filtering feature does not work for ipv6 sessions.
This issue is seen only when **ipv6 cef** is enabled on the PDSN.
Workaround: disable **ipv6 cef** on the PDSN.
- CSCsb61054—Periodic Accounting Interval Wrong When Using Broadcast Accounting
On Cisco router running 12.3(14)YX Packet Data Serving Node (PDSN), when AAA broadcast accounting is used in conjunction with periodic accounting, the periodic accounting interval will be n times slower than configured, where n is the number of servers in the broadcast accounting list.
The workaround is to.
Workaround: compensate by configuring a periodic interval $1/n$ times the desired interval.

Unresolved Caveats Prior to Cisco IOS 12.3(14)YX

The following caveats are unresolved in Cisco IOS Release 12.3(11)YF3:

- CSCee74242—Flow Count Incorrect When Prepaid Flows Get Deleted
Total flow count displayed in the **show cdma pdsn** output does not match the actual number of flows present on the box.
This occurs only for prepaid sessions on Cisco PDSN.
Workaround: none.
- CSCef31289—Unsupported Attr Debugs While Opening Sessions in PDSN
On a Cisco PDSN running the Cisco IOS 12.3(8)XW R2.0 PDSN image, on opening a session with radius debugs enabled, the “AAA Unsupported Attr” debug messages are printed even though no functionality is affected.
Workaround: none.
- CSCef36788—Downstream Throughput Lower Than Expected Number by 10%
Downstream packet throughput for the Cisco PDSN R2.0 release has degraded. Throughput on the 7200 NPE-G1 and MWAM platform is 10% lower than target numbers.
This condition occurs when packet size is 512 Bytes and traffic is pumped on all 20K sessions.
Workaround: none.
- CSCef39494—Prepaid MIP Flow Not Deleted on Quota Expiry
On a Cisco router running Release 2.0 PDSN software, when multiple prepaid flows are opened for the same user and traffic is sent through a single flow so as to cross the threshold and quota granted, the PDSN does not close the flow. However, traffic through the flow is not switched as expected.
This symptom occurs when prepaid accounting is enabled, and multiple Mobile IP prepaid flows are opened for the same user.
Workaround: none.
- CSCef40729—Session is Not Cleared in PDSN With Tunnel Scalability Turned Off
A Mobile IP session, created with UDP tunneling between the HA and PDSN, does not get cleared when the session is closed from MN.
Workaround: use other modes of tunneling like, IPINIP or GRE between the PDSN and HA.

- CSCef40742—PDSN Accepts Value 0 for cCdmaSessionPdsnMaxFailHistory from NMS.

On a Cisco router running R2.0 Packet Data Serving Node (PDSN) Software, the CISCO-CDMA-PDSN-MIB counter cCdmaSessionPdsnMaxFailHistory accepts a value of zero (0) when configured through NMS.

Workaround: none.
- CSCef54687—Incorrect Disconnect Reason Send For Prepaid PMIP Flow

On a Cisco router running Release 2.0 PDSN software, for a volume based prepaid proxy mobile IP flow with resource revocation enabled, when the PDSN deletes prepaid flow on receiving the resource revocation request from the HA, the PDSN sets the “disconnect reason” as “client service termination” instead of “remote forced disconnect” in online access-request.

This symptom occurs for revocation enabled proxy mobile IP prepaid flows alone.

Workaround: none.
- CSCef61626—MSID Flow is Opened When Quota Provided Has Both Volume and Duration Attribute

On a Cisco router running Release 2.0 PDSN software, an MSID flow is opened when the quota allocated by HAAA has both volume and duration attributes

This symptom only occurs for MSID flows.

Workaround: none.
- CSCef61637—MSID Flow is Opened For Undefined PPAC

On a Cisco Router running Release 2.0 PDSN software, an MSID flow is opened without prepaid capability when the **SelectedforSession** attribute has an incorrect value and PPAQ value is received in Access Accept.

The session should have been terminated in this case.

This symptom occurs for msid flow, when the SelectedforSession attribute has an incorrect value and PPAQ value is received in Access Accept.

Workaround: none.
- CSCef64126—CDMA IPSec Support for VRF and HA-SLB.

Cisco PDSN Release 2.0 currently supports CDMA IPSec only for non-VRF MIP flows. The PDSN needs to support CDMA IPSec for VRF flows also.

Workaround: none.
- CSCef68963—Incorrect CISCO-MOBILE-IP-MIB Counter Values

On a Cisco router running R2.0 Packet Data Serving Node (PDSN) or Home Agent Software, the CISCO-MOBILE-IP-MIB counters “cmiFaRegVisitorRegFlagsRev1” and “cmiSecAssoc” table entries show incorrect values.

Workaround: none.
- CSCef92130—CDMA IPSec Fails When Packets Are Sent Over Different Interface

On a Cisco Router running PDSN R2.0 software with CDMA IPSec configured, if the outgoing interface is changed (example due to OSPF cost), then packets from PDSN go unencrypted.

Workaround: ensure that all MIP packets are sent over the interface on which crypto maps get applied. For interface redundancy, port channel configuration may be used.

- CSCeg83033—G1 and G16 Counter Value Mismatch When Compliance IS835c Configured

On a Cisco router running Release 2.1 PDSN software, with the **cdma pdsn compliance is835c account ipmobile control-packets** CLI configured to account for Mobile IP control packets on G1 and G2 counters, the values displayed on G1 and G16 do not match.

This issue occurs on R2.1 PDSN images. Opening a MIP flow, we found that the values displayed on G1 and G16 do not match. Given that, there is no traffic sent through the flow, these values should be the same.

Workaround: none.
- CSCin75685—A11 Update Other Reason Incorrect For Closed RP Session Open/Close

When a closed RP session is opened and closed on the Packet Data Service Node (PDSN), the statistics counter update reason “other” shows invalid value.

This condition is seen only when a closed RP session is opened and closed

Workaround: none. Since the A11 update counter is not used for closed RP sessions on the PDSN, this counter can be ignored.
- CSCin78778—Session-down Counter Increments Even When There is no Session

On a Cisco router running PDSN R2.0 image configured as Cluster Controller, the Session-down counter is incremented even if there are no active sessions on any of its members.

Workaround: none.
- CSCin78831—Cluster Member Displayed Twice in show Command Display

Cluster members are displayed twice in the show cdma pdsn cluster controller member load command.

This condition occurs only when all members except one are removed from the controller.

Workaround: none.
- CSCin85270—IPsec Tunnel Torn Down Before Revocation Completion for PMIP Session

The Cisco PDSN closes the IPsec tunnel and cannot decrypt and process revocation acknowledgements from the Home Agent under the following scenario:

 - CDMA IPsec is enabled on the PDSN.
 - Revocation is triggered on the PDSN for a proxy mobileip session.
 - No more mobiles are connected to the corresponding Home Agent (i.e., the PDSN closes the mobileip tunnel)

Workaround: none. This is a cosmetic issue; it happens rarely and not processing revocation acknowledgements does not break any functionality.
- CSCin88147—Traceback Found While PDSN Cluster Controller CLI

On a Cisco router running PDSN software, traceback is found while configuring the **cdma pdsn cluster controller interface interface-name** command.

This issue occurs under the following conditions:

 - a. Configure the HSRP ACTIVE/STANDBY in the controllers.
 - b. Configure the cluster in both the controllers.

Workaround: none.

- **CSCin88503—PDSN Crashed During Handoff**

Cisco PDSN running 12.3(11)YF image may crash while handoff of a session happens from one PCF to another.

This issue occurs during a PCF to PCF handoff; however, this is a rare condition.

Workaround: issue the **cdma pdsn compliance is835a handoff** command.
- **CSCin94219—ClosedRP PDSN Reloads During CRP tunnel Going Down**

Cisco PDSN enabled for Closed RP feature reloads, when the Closed RP PCF opens multiple L2TP tunnels with the PDSN and distributes the Closed RP sessions among these L2TP tunnels.

Workaround: none.
- **CSCsa44570—PDSN Member Info Not Synching With Standby Controller.**

On Cisco router running Release 2.0 PDSN software, the PDSN Member Info is not getting synched from the active to the standby PDSN controller if the **redundancy inter-device** command has been configured on the controller. This rules out the possibility of configuring the ODAP server redundancy on the PDSN controllers.

This behavior is seen only if the **redundancy inter-device** command has been configured on the processor. The PDSN controller redundancy works fine if this CLI is not configured on the processor.

Workaround: do not configure ODAP server redundancy on the controllers.
- **CSCsa79410—PDSN MIP Client Upload Fails With Large IP Packet**

When uploading files from a Mobile IP client to a server through the PDSN, packets that are larger than 1480 bytes (and the DF bit is set) are dropped by the PDSN. The PDSN does not send ICMP UNFRAG error to MIP client, and fails to learn the smaller mtu path. The MIP client will continue to send packets larger than 1480 and it will never get to the server. SIP clients are not affected.

The IP MTU setting for the IP/IP tunnel between the FA and HA is 1480 bytes.

Workaround: issue the **no ip mobile tunnel path-mtu-discovery** command to disable path MTU discovery on the PDSN.
- **CSCsb29278—Tracebacks Seen With Active Controller.**

On Cisco router running R2.1 PDSN software, the active controller was idle for sometime, and suddenly the following traceback was seen:

```
tb1-7600a-cont1#
Jun 24 23:51:27.327: %SCHED-3-STUCKTMR: Sleep with expired timer 221E9418, time
0xAC91BF0 (00:00:00 ago).
-Process= "masterPdsn", ipl= 5, pid= 137
-Traceback= 20698F7C 20799884 20799C54 2036C51C
```

Workaround: none.
- **CSCsb30480—Out-of-Sequence Acct-Response Packets Triggers Interim Accounting**

On a Cisco router running R2.1 PDSN software, after a dormant handoff, the PDSN sends “watchdog” packets to the Radius Server periodically in a scenario where the Accounting-response received from the Radius server are out of sequence.

This Issue occurs during dormant handoffs, only if the “Accounting-Response” for Accounting-Stop was received first, followed by Accounting-Response for Accounting-Start.

Workaround: none.

- CSCsb39828—PDSN Sends Packets Out Of Sequence When MPPC Compression is Enabled
A Cisco router running PDSN software will send MPPC compressed packets out of sequence towards a client.
This condition occurs when MPPC compression is enabled on the PDSN.
Workaround: alternate compression methods such as STAC can be used, or data can be sent uncompressed.
- CSCsb40378—PDSN Crash During Session Deletion
A crash may occur on the PDSN running IOS 12.3(11)T3 resulting in “System returned to ROM by bus error.”
Workaround: none.

Unresolved Caveats Prior to Cisco IOS Release 12.3(11)YF3

The following caveats are unresolved in Cisco IOS Release 12.3(11)YF2:

- CSCee74242—Flow Count Incorrect When Prepaid Flows Get Deleted
Total flow count displayed in the **show cdma pdsn** output does not match the actual number of flows present on the box.
This occurs only for prepaid sessions on Cisco PDSN.
Workaround: none.
- CSCef36788—Downstream Throughput Lower Than Expected Number by 10%
Downstream packet throughput for the Cisco PDSN R2.0 release has degraded. Throughput on the 7200 NPE-G1 and MWAM platform is 10% lower than target numbers.
This condition occurs when packet size is 512 Bytes and traffic is pumped on all 20K sessions.
Workaround: none.
- CSCef39342—Non-Crypto Packets Dropped Due to CDMA and CLI IPSEC Interoperability
When CDMA IPsec is configured on the PDSN and CLI IPsec is configured on the HA, in the absence of a IPsec user MIP tunnel, normal IP traffic is dropped because no crypto tunnel is established between PDSN and HA.
This symptom has been observed on the PDSN and HA routers running Cisco IOS release 12.3T.
Workaround: none.
- CSCef39494—Prepaid MIP Flow Not Deleted on Quota Expiry
On a Cisco router running Release 2.0 PDSN software, when multiple prepaid flows are opened for the same user and traffic is sent through a single flow so as to cross the threshold and quota granted, the PDSN does not close the flow. However, traffic through the flow is not switched as expected.
This symptom occurs when prepaid accounting is enabled, and multiple Mobile IP prepaid flows are opened for the same user.
Workaround: none.
- CSCef40729—Session is Not Cleared in PDSN With Tunnel Scalability Turned Off
A Mobile IP session, created with UDP tunneling between the HA and PDSN, does not get cleared when the session is closed from MN.
Workaround: use other modes of tunneling like, IPINIP or GRE between the PDSN and HA.

- CSCef40742—PDSN Accepts Value 0 for cCdmaSessionPdsnMaxFailHistory From NMS.
On a Cisco router running R2.0 Packet Data Serving Node (PDSN) software, the CISCO-CDMA-PDSN-MIB counter “cCdmaSessionPdsnMaxFailHistory” accepts a value of zero when configured through NMS.
Workaround: none.
- CSCef54687—Incorrect Disconnect Reason Send For Prepaid PMIP Flow
On a Cisco router running Release 2.0 PDSN software, for a volume based prepaid proxy mobile IP flow with resource revocation enabled, when the PDSN deletes prepaid flow on receiving the resource revocation request from the HA, the PDSN sets the “disconnect reason” as “client service termination” instead of “remote forced disconnect” in online access-request.
This symptom occurs for revocation enabled proxy mobile IP prepaid flows alone.
Workaround: none.
- CSCef61626—MSID Flow is Opened When Quota Provided Has Both Volume and Duration Attribute
On a Cisco router running Release 2.0 PDSN software, an MSID flow is opened when the quota allocated by HAAA has both volume and duration attributes
This symptom only occurs for MSID flows.
Workaround: none.
- CSCef61637—MSID Flow is Opened For Undefined PPAC
On a Cisco Router running Release 2.0 PDSN software, an MSID flow is opened without prepaid capability when the **SelectedforSession** attribute has an incorrect value and PPAQ value is received in Access Accept.
The session should have been terminated in this case.
This symptom occurs for msid flow, when the SelectedforSession attribute has an incorrect value and PPAQ value is received in Access Accept.
Workaround: none.
- CSCef75738—PDSN Rejects an RRQ With Active Stop If Prior Record Not Start/stop
Rp counters are not incrementing in a Cisco router running 12.3T R2.0 Release PDSN software.
The PDSN rejects an RRQ with Active Stop if a prior record is not started or stopped.
Workaround: none.
- CSCin75685—A11 Update Other Reason Incorrect For Closed RP Session Open/Close
When a closed RP session is opened and closed on the Packet Data Service Node (PDSN), the statistics counter update reason “other” shows invalid value.
This condition is seen only when a closed RP session is opened and closed
Workaround: none. Since the A11 update counter is not used for closed RP sessions on the PDSN, this counter can be ignored.

- CSCin85270—IPsec Tunnel Torn Down Before Revocation Completion for PMIP Session

The Cisco PDSN closes the IPsec tunnel and cannot decrypt and process revocation acknowledgements from the Home Agent under the following scenario:

- CDMA IPsec is enabled on the PDSN.
- Revocation is triggered on the PDSN for a proxy mobileip session.
- No more mobiles are connected to the corresponding Home Agent (i.e., the PDSN closes the mobileip tunnel)

Workaround: none. This is a cosmetic issue; it happens rarely and not processing revocation acknowledgements does not break any functionality.

Unresolved Caveats Prior to Cisco IOS Release 12.3(11)YF2

The following caveats are unresolved in Cisco IOS Release 12.3(11)YF1:

- CSCee74242—Flow Count Incorrect When Prepaid Flows Get Deleted

Total flow count displayed in the **show cdma pdsn** output does not match the actual number of flows present on the box.

This occurs only for prepaid sessions on Cisco PDSN.

Workaround: none.

- CSCef36788—Downstream Throughput Lower Than Expected Number by 10%

Downstream packet throughput for the Cisco PDSN R2.0 release has degraded. Throughput on the 7200 NPE-G1 and MWAM platform is 10% lower than target numbers.

This condition occurs when packet size is 512 Bytes and traffic is pumped on all 20K sessions.

Workaround: none.

- CSCef39342—Non-Crypto Packets Dropped Due to CDMA and CLI IPSEC Interoperability

When CDMA IPsec is configured on the PDSN and CLI IPsec is configured on the HA, in the absence of a IPsec user MIP tunnel, normal IP traffic is dropped because no crypto tunnel is established between PDSN and HA.

This symptom has been observed on the PDSN and HA routers running Cisco IOS release 12.3T.

Workaround: none.

- CSCef39494—Prepaid MIP Flow Not Deleted on Quota Expiry

On a Cisco router running Release 2.0 PDSN software, when multiple prepaid flows are opened for the same user and traffic is sent through a single flow so as to cross the threshold and quota granted, the PDSN does not close the flow. However, traffic through the flow is not switched as expected.

This symptom occurs when prepaid accounting is enabled, and multiple Mobile IP prepaid flows are opened for the same user.

Workaround: none.

- CSCef40729—Session is Not Cleared in PDSN With Tunnel Scalability Turned Off

A Mobile IP session, created with UDP tunneling between the HA and PDSN, does not get cleared when the session is closed from MN.

Workaround: use other modes of tunneling like, IPINIP or GRE between the PDSN and HA.

- CSCef40742—PDSN Accepts Value 0 for cCdmaSessionPdsnMaxFailHistory From NMS.
On a Cisco router running R2.0 Packet Data Serving Node (PDSN) software, the CISCO-CDMA-PDSN-MIB counter “cCdmaSessionPdsnMaxFailHistory” accepts a value of zero when configured through NMS.
Workaround: none.
- CSCef54687—Incorrect Disconnect Reason Send For Prepaid PMIP Flow
On a Cisco router running Release 2.0 PDSN software, for a volume based prepaid proxy mobile IP flow with resource revocation enabled, when the PDSN deletes prepaid flow on receiving the resource revocation request from the HA, the PDSN sets the “disconnect reason” as “client service termination” instead of “remote forced disconnect” in online access-request.
This symptom occurs for revocation enabled proxy mobile IP prepaid flows alone.
Workaround: none.
- CSCef61626—MSID Flow is Opened When Quota Provided Has Both Volume and Duration Attribute
On a Cisco router running Release 2.0 PDSN software, an MSID flow is opened when the quota allocated by HAAA has both volume and duration attributes
This symptom only occurs for MSID flows.
Workaround: none.
- CSCef61637—MSID Flow is Opened For Undefined PPAC
On a Cisco Router running Release 2.0 PDSN software, an MSID flow is opened without prepaid capability when the **SelectedforSession** attribute has an incorrect value and PPAQ value is received in Access Accept.
The session should have been terminated in this case.
This symptom occurs for msid flow, when the SelectedforSession attribute has an incorrect value and PPAQ value is received in Access Accept.
Workaround: none.
- CSCef75738—PDSN Rejects an RRQ With Active Stop If Prior Record Not Start/stop
Rp counters are not incrementing in a Cisco router running 12.3T R2.0 Release PDSN software.
The PDSN rejects an RRQ with Active Stop if a prior record is not started or stopped.
Workaround: none.
- CSCin75685—A11 Update Other Reason Incorrect For Closed RP Session Open/Close
When a closed RP session is opened and closed on the Packet Data Service Node (PDSN), the statistics counter update reason “other” shows invalid value.
This condition is seen only when a closed RP session is opened and closed
Workaround: none. Since the A11 update counter is not used for closed RP sessions on the PDSN, this counter can be ignored.

- CSCin85270—IPsec Tunnel Torn Down Before Revocation Completion for PMIP Session
The Cisco PDSN closes the IPsec tunnel and cannot decrypt and process revocation acknowledgements from the Home Agent under the following scenario:
 - CDMA IPsec is enabled on the PDSN.
 - Revocation is triggered on the PDSN for a proxy mobileip session.
 - No more mobiles are connected to the corresponding Home Agent (i.e., the PDSN closes the mobileip tunnel)

Workaround: none. This is a cosmetic issue; it happens rarely and not processing revocation acknowledgements does not break any functionality
- CSCin86601—PDSN A11 Session Update Retransmission is not Working Correctly
The Cisco PDSN is not taking the configured a11 session update timeout value into consideration while retransmitting the a11 session update message.
This condition occurs when the Cisco router is configured for PDSN.
Workaround: none.
- CSCin86667—SDB Airlink Record Rejected After Dormant Handoff
When an SDB airlink record is received after a SETUP/START airlink record, the RRQ is rejected with an error code of 86H, with the following debug printed:
“Bad Airlink record. Received SDB airlink after SETUP/START”.
Workaround: none.
- CSCin86716—PDSN to Parse SDB Records as per IOS 4.x
The Cisco PDSN cannot parse A11 Registration request message from a PCF that contains attribute value 32 in SDB airlink record.
This condition occurs when the PCF sends attribute value 32 in the SDB airlink record.
Workaround: none.

Unresolved Caveats Prior to Cisco IOS Release 12.3(11)YF1

The following caveats are unresolved in Cisco IOS Release 12.3(11)YF:

- CSCee74242—Flow Count Incorrect When Prepaid Flows Get Deleted
Total flow count displayed in the **show cdma pdsn** output does not match the actual number of flows present on the box.
This occurs only for prepaid sessions on Cisco PDSN.
Workaround: none.
- CSCef36788—Downstream Throughput Lower Than Expected Number by 10%
Downstream packet throughput for the Cisco PDSN R2.0 release has degraded. Throughput on the 7200 NPE-G1 and MWAM platform is 10% lower than target numbers.
This condition occurs when packet size is 512 Bytes and traffic is pumped on all 20K sessions.
Workaround: none.

- CSCef39342—Non-Crypto Packets Dropped Due to CDMA and CLI IPSEC Interoperability
When CDMA IPsec is configured on the PDSN and CLI IPsec is configured on the HA, in the absence of a IPsec user MIP tunnel, normal IP traffic is dropped because no crypto tunnel is established between PDSN and HA.
This symptom has been observed on the PDSN and HA routers running Cisco IOS release 12.3T.
Workaround: none.
- CSCef39494—Prepaid MIP Flow Not Deleted on Quota Expiry
On a Cisco router running Release 2.0 PDSN software, when multiple prepaid flows are opened for the same user and traffic is sent through a single flow so as to cross the threshold and quota granted, the PDSN does not close the flow. However, traffic through the flow is not switched as expected.
This symptom occurs when prepaid accounting is enabled, and multiple Mobile IP prepaid flows are opened for the same user.
Workaround: none.
- CSCef40729—Session is Not Cleared in PDSN With Tunnel Scalability Turned Off
A Mobile IP session, created with UDP tunneling between the HA and PDSN, does not get cleared when the session is closed from MN.
Workaround: use other modes of tunneling like, IPINIP or GRE between the PDSN and HA.
- CSCef40742—PDSN Accepts Value 0 for cCdmaSessionPdsnMaxFailHistory From NMS.
On a Cisco router running R2.0 Packet Data Serving Node (PDSN) software, the CISCO-CDMA-PDSN-MIB counter “cCdmaSessionPdsnMaxFailHistory” accepts a value of zero when configured through NMS.
Workaround: none.
- CSCef43555—PDSN Sends Wrong Counter When cCdmaPcfSoRpUpdOtherReaReqs is Requested
On a Cisco router running R2.0 PDSN software, the CISCO-CDMA-PDSN-MIB counter cCdmaPcfSoRpUpdOtherReaReqs shows incorrect values.
Workaround: none.
- CSCef54687—Incorrect Disconnect Reason Send For Prepaid PMIP Flow
On a Cisco router running Release 2.0 PDSN software, for a volume based prepaid proxy mobile IP flow with resource revocation enabled, when the PDSN deletes prepaid flow on receiving the resource revocation request from the HA, the PDSN sets the “disconnect reason” as “client service termination” instead of “remote forced disconnect” in online access-request.
This symptom occurs for revocation enabled proxy mobile IP prepaid flows alone.
Workaround: none.
- CSCef57647—Incorrect PDSN CISCO-CDMA-PDSN-MIB Counter Values
On a Cisco router running R2.0 Packet Data Serving Node (PDSN) software, the CISCO-CDMA-PDSN-MIB counters “cCdmaActiveSessions”, “cCdmaDormantSessions”, and “cCdmaPcfSoRpUpdOtherReaReqs” show incorrect values.
Workaround: none.

- CSCef61626—MSID Flow is Opened When Quota Provided Has Both Volume and Duration Attribute
On a Cisco router running Release 2.0 PDSN software, an MSID flow is opened when the quota allocated by HAAA has both volume and duration attributes
This symptom only occurs for MSID flows.
Workaround: none.
- CSCef61637—MSID Flow is Opened For Undefined PPAC
On a Cisco Router running Release 2.0 PDSN software, an MSID flow is opened without prepaid capability when the **SelectedforSession** attribute has an incorrect value and PPAQ value is received in Access Accept.
The session should have been terminated in this case.
This symptom occurs for msid flow, when the SelectedforSession attribute has an incorrect value and PPAQ value is received in Access Accept.
Workaround: none.
- CSCef75730—RP Counters are Not Incremented When Different GRE With No Setup
Rp counters are not incrementing in a Cisco router running 12.3T R2.0 Release PDSN software. RP counters and poorly formed Request are not incrementing in the PDSN.
The RP counters in the PDSN are not incremented when a different GRE with no setup was sent by simulator.
Workaround: none.
- CSCef75738—PDSN Rejects an RRQ With Active Stop If Prior Record Not Start/stop
Rp counters are not incrementing in a Cisco router running 12.3T R2.0 Release PDSN software.
The PDSN rejects an RRQ with Active Stop if a prior record is not started or stopped.
Workaround: none.
- CSCef86875—PDSN Reloads While Disabling Conditional Debugging For Prepaid
On Cisco router running Release 2.1 PDSN software, the router reloads while disabling conditional debugging feature for Prepaid Accounting.
The symptom occurs when prepaid accounting is enabled with conditional debugging.
Workaround: none.
- CSCef92130—CDMA IPSec Fails When Packets Are Sent Over Different Interface
On a Cisco Router running PDSN R2.0 software with CDMA IPSec configured, if the outgoing interface is changed (example due to OSPF cost), then packets from PDSN go unencrypted.
Workaround: ensure that all MIP packets are sent over the interface on which crypto maps get applied. For interface redundancy, port channel configuration may be used.

- CSCin85270—IPsec Tunnel Torn Down Before Revocation Completion For PMIP Session
PDSN closes IPsec tunnel and so cannot decrypt and process revocation acknowledgements from Home Agent under the following conditions:
 - CDMA IPsec is enabled on PDSN.
 - Revocation is triggered on PDSN for a proxy mobileip session.
 - No more mobiles are connected to the corresponding Home Agent (for example, the PDSN closes the mobileip tunnel).

Workaround: none. This is a cosmetic issue, as it happens rarely and not processing revocation acknowledgement does not break any functionality
- CSCsa44772—PDSN Should Not Send A11 Session UPD if Current RNPDIIT <= prev RNPDIIT
The PDSN sends a session update message to the PCF when RN-PDIIT downloaded <= RN-PDIIT stored.
This condition occurs when the second MIP flow is opened for a user and the same RN-PDIIT, Always-On values are downloaded from RADIUS server.
Workaround: none.
- CSCsa45264—Last Character of Calling Station ID Stripped When PDSN Sends to LNS
On Cisco PDSN running 12.3(8)XW03, when VPDN flows are opened on the A11 session, the PDSN acting as LAC will send an ICRQ to the LNS. In the ICRQ message PDSN will include the Calling Station ID received in the A11 Registration Request. When the Calling Station ID is sent from PDSN, the last character of Calling Station ID is not encoded in the ICRQ to the LNS.
This condition occurs for all VPDN flows opened over the A11 session.
Workaround: none.

Unresolved Caveats Prior to Cisco IOS Release 12.3(11)YF

The following caveats are unresolved in Cisco IOS Release 12.3(8)XW3

- CSCed65017—MWAM: Config CLI That Fail Batch Mode Copy Fail Config-mode SUP
Some configuration commands fail, do not operate properly, or cause dead memory when using batch mode config download or config-mode supervisor.
This problem occurs when the MWAM processor is configured for **supervisor** config-mode.
Workaround: Use config-mode local on MWAM.
- CSCef64126—CDMA IPsec Support for VRF and HA-SLB.
Cisco PDSN Release 2.0 currently supports CDMA IPsec only for non-VRF MIP flows. The PDSN needs to support CDMA IPsec for VRF flows also.
Workaround: none.
- CSCef75989—**ip radius source-interface** Command not Working
On a Cisco router running R2.0 Home Agent Software 12.3(8)XW, the **ip radius source-interface** command does not work. Even if you configure **ip radius source-interface xyz**, the router still sends the address of the physical interface connected to the radius server, rather than the interface configured in the command (*xyz*).
Workaround: Configure the **ip radius source-interface** at the server-group level.

- CSCef79940—Unable to Configure CLI **radius-server attribute 44 include-in-access**

On a Cisco PDSN running the 12.3(8)XW R2.0 PDSN image on MWAM platform, configuring the **radius-server attribute 44 include-in-access-req** command, or the **ip rad source-interface** command causes an error message “% Can't insert AAA config node for vrf=”, if the **aaa accounting system default start-stop** command is configured on the MWAM, and the MWAM config mode is the supervisor mode.

Workaround: This issue is not seen if the configuration **aaa accounting system default start-stop** command is not configured on the MWAM or if the MWAM config mode is local.
- CSCef92130—CDMA IPSec Fails When Packets Are Sent Over Different Interface

On a Cisco Router running PDSN R2.0 software with CDMA IPSec configured, MIP flows will not come up if the Mobile IP tunnel endpoint is different that of IPSec tunnel end point. This issue is seen only for MIP flows, and not for PMIP flows.

Workaround: Configure the IPSec tunnel end point as the MIP tunnel end point.

Unresolved Caveats Prior to Cisco IOS Release 12.3(8)XW3

The following caveats are unresolved in Cisco IOS Release 12.3(8)XW2

- CSCed86177—Tracebacks Found on PDSN with CEF and NAT Enabled for SIP Flow

A Cisco router running 12.3T R2.0 Release PDSN software, sometimes produces tracebacks while sending bidirectional traffic from mobile node to the reflector in SIP flow with compress stack enabled and cef switched.

Workaround: none.
- CSCee13372—IPSec Tunnel Goes Down Before Receiving ACK for Revocation Request

When the last mobile tunnel binding is brought down on the Cisco HA, a revocation message is sent from the HA and the CDMA IPSec tunnel is brought down without waiting for a revocation acknowledgement message from the PDSN.

This symptom has been observed on a router that is running Cisco IOS release 12.3T software.

Workaround: none.
- CSCee74242—Flow Count Incorrect When Prepaid Flows Get Deleted

Total flow count displayed in **show cdma pdsn** output does not match the actual number of flows present on the box.

This occurs only for prepaid sessions on Cisco PDSN.

Workaround: none.
- CSCef27300—Framed-IP-Addr Attr Not Sent When Both RADIUS and CDMA CLI Configured

Framed-IP-Address in the Access-Request for MIP flows is not sent even if the **ip mobile foreign-agent send-mn-address** command is configured on the Cisco PDSN (PDSN) and Home Agent (HA).

The **radius-server attribute 8 include-in-access-req** command is also configured along with CLI **ip mobile foreign-agent send-mn-address**, and it is not sending the “Framed-IP-Addr” attribute in its Access Request to AAA.

Workaround: unconfigure the **radius-server attribute 8 include-in-access-req** command on the box.

- CSCef31289—Unsupported Attr Debugs While Opening Sessions in PDSN

On a Cisco PDSN running the Cisco IOS 12.3(8)XW R2.0 PDSN image, on opening a session with radius debugs enabled, the “AAA Unsupported Attr” debug messages are printed even though no functionality is affected.

Workaround: none.
- CSCef36788—Downstream Throughput Lower Than Expected Number by 10%

Downstream packet throughput for Cisco PDSN R2.0 release has degraded. Throughput on 7200 NPE-G1 and MWAM platform is 10% lower than target numbers.

The following conditions exist for this problem: packet size is 512 Bytes and traffic is pumped on all 20K sessions.

Workaround: none.
- CSCef39342—Non-Crypto Packets Dropped Due to CDMA and CLI IPSec Interoperability

When CDMA IPSec is configured on PDSN and CLI IPSec is configured on HA, in the absence of IPSec user MIP tunnel, normal IP traffic is dropped as no crypto tunnel is established between PDSN and HA.

This symptom has been observed on PDSN and HA routers that are running Cisco IOS release 12.3T.

Workaround: none.
- CSCef39494—Prepaid MIP Flow Not Deleted on Quota Expiry

On a Cisco router running Release 2.0 PDSN software, when multiple prepaid flows are opened for the same user and traffic is sent through a single flow so as to cross the threshold and quota granted, the PDSN does not close the flow. However, traffic through the flow is not switched as expected.

This symptom occurs when prepaid accounting is enabled and multiple mobile IP prepaid flows are opened for the same user.

Workaround: none.
- CSCef40729—Session is Not Cleared in PDSN With Tunnel Scalability Turned Off

A mobile IP session, created with UDP tunneling between the HA and PDSN, does not get cleared when the session is closed from MN.

Workaround: Use other modes of tunneling like, IPINIP or GRE between PDSN and HA.
- CSCef40742—PDSN Accepts Value 0 for cCdmaSessionPdsnMaxFailHistory from NMS.

On a Cisco router running R2.0 Packet Data Serving Node (PDSN) Software, the CISCO-CDMA-PDSN-MIB counter cCdmaSessionPdsnMaxFailHistory accepts a value of zero (0) when configured through NMS.

Workaround: none.
- CSCef43555—PDSN Sends Wrong Counter When cCdmaPcfSoRpUpdOtherReaReqs is Requested

On a Cisco router running R2.0 PDSN Software, the CISCO-CDMA-PDSN-MIB counter cCdmaPcfSoRpUpdOtherReaReqs show incorrect values.

Workaround: none.

- CSCef50548—TOS Value Set to Non-zero Value for PPP Control Packets

On Cisco router running Release 2.0 PDSN software, during Point-to-Point (PPP) negotiation, the IPCP control packets sent downstream to the Mobile Node from PDSN are encapsulated using GRE and then sent to Mobile Node. The DSCP marking on Type of Service (TOS) filed in the outer header, found be a non-zero (Garbage) value.

This behavior is seen only when the PPP negotiations happens.If traffic is sent over the established tunnel, those packets are marked with correct (TOS =0) value.

Workaround: none.

- CSCef54687—Incorrect Disconnect Reason Send For Prepaid PMIP Flow

On a Cisco router running Release 2.0 PDSN software for a volume-based prepaid proxy mobile IP flow with resource revocation enabled, when the PDSN deletes a prepaid flow on receiving the resource revocation request from the HA, the PDSN sets the “disconnect reason” as “client service termination” instead of “remote forced disconnect” in online access-request.

This condition occurs for revocation enabled proxy mobile IP prepaid flows alone

Workaround: none.

- CSCef66797—Accounting ON/OFF Message Not Sent Upon Processor Reload

On Cisco router running Release 2.0 PDSN software, upon reload of the MWAM processor where the PDSN is loaded, the Accounting OFF message is not sent towards the AAA. Also the Accounting ON message is not sent when the processor comes up after reload.

This problem exists under the following conditions:

- both the Accounting ON/OFF message is not sent if the MWAM Config-mode is set to Supervisor.
- If the MWAM Config-mode is set to local, then the Accounting ON message alone sent after the processor comes up, whereas the Accounting OFF message is not sent after the reload.

Workaround: Include the “Broadcast” keyword in the following accounting configuration of PDSN:

aaa accounting system default start-stop broadcast group *group name*.

Additionally, the MWAM config-mode should be set to “Local”.

- CSCef61626—MSID Flow is Opened When Quota Provided Has Both Vol and Dur Attribute

On a Cisco Router running Release 2.0 PDSN Software, the MSID flow is opened when the quota allocated by HAAA has both volume and duration attributes.

This symptom only occurs for MSID flows.

Workaround: none.

- CSCef61637—MSID Flow is Opened For Undefined PPAC

On a Cisco Router running Release 2.0 PDSN Software, a MSID flow is opened without prepaid capability when the “SelectedforSession” attribute has an incorrect value, and the PPAQ value is received in Access Accept.

In this case, the session should have been terminated.

This symptom occurs for MSID flows when the “SelectedforSession” attribute has an incorrect value and PPAQ value is received in Access Accept.

Workaround: none.

- CSCef68963—Incorrect CISCO-MOBILE-IP-MIB Counter Values

On a Cisco router running R2.0 Packet Data Serving Node (PDSN) or Home Agent Software, the CISCO-MOBILE-IP-MIB counters “cmiFaRegVisitorRegFlagsRev1” and “cmiSecAssoc” table entries show incorrect values.

Workaround: none.

- CSCin77744—PDSN Drops Fragmented PCF Packets Intermittently

On the Packet Data Service Node (PDSN), when the Generic Routing Encapsulation (GRE) packets received from the Packet Control Function (PCF), they are dropped intermittently, if these packets are fragmented.

Packets drops are seen on the PDSN when the PPP negotiation between the PDSN and Mobile Node Terminates the Compression Control Protocol (CCP) and then during the data transfer the Mobile Node sends another CCP ConfReq to the PDSN.

Workaround: by disabling compression on PDSN Virtual Template packet drop was not observed

- CSCin78778—Session-down Counter Increments Even When There is no Session

On a Cisco router running PDSN R2.0 image configured as Cluster Controller, the Session-down counter is incremented even if there are no active sessions on any of its members.

Workaround: none.

- CSCin78831—Cluster Member Displayed Twice in **show** Command Display

Cluster members are displayed twice in the **show cdma pdsn cluster controller member load** command. This condition occurs only when all members except one are removed from the controller.

Workaround: none.

- CSCin79106—Mismatch in Session Count in Cluster Controller

On a Cisco router running the PDSN R2.0 image, a mismatch of cluster statistics is encountered. Statistics of the total number of sessions displayed in the **show cdma pdsn cluster controller member load** command do not match with statistics of the **show cdma pdsn cluster controller session count** command.

Workaround: none.

- CSCin81236—Conditional Debugging Skips Some RADIUS Msgs for MIP Flows

When conditional debugging is enabled on Cisco PDSN running Cisco IOS 12.3(8)XW image, RADIUS related debugs are not shown sometimes for a Mobile IP flow that is opened on the box.

This condition occurs when conditional debugging is set for RADIUS related debugs.

Workaround: none.

- CSCin81520—Extra Mobile IP Debugs are Printed For Conditional Debugging
Some extra mobile IP debugs are printed on a Cisco PDSN, running Cisco IOS 12.3(08)XW software, when mobile IP conditional debugging is enabled on it. Debugs that get printed are not corresponding to the user.
This condition occurs when conditional debugging for mobile IP is turned on.
Workaround: none.

Unresolved Caveats Prior to Cisco IOS Release 12.3(8)XW2

The following caveats are unresolved in Cisco IOS Release 12.3(8)XW

- CSCed86177—Tracebacks Found on PDSN While Opening Simple IP Session (Simple IP session)
Cisco routers running Packet Data Serving Node software may show traceback when the compression stack is enabled while opening simple IP sessions.
Workaround: none.
- CSCee13372—IPSec Tunnel Goes Down Before Receiving ACK for Revocation Request (Resource Revocation)
On clearing the IP mobile bindings manually on PDSN, ipsec tunnel goes down before waiting for the acknowledgement for the Resource Revocation from HA
This condition is observed under the following conditions
 - a. Clear the ip mobile bindings manually on PDSN,
 - b. PDSN sends Resource revocation message to HA.
 - c. IPSec tunnel goes down before ACK from HA.**Workaround:** none.
- 3. CSCed86144—Tracebacks Found in Clustering (Clustering)
A Cisco router running Packet Data Serving Node (PDSN) software in cluster controller member environment may show tracebacks on backup controller.
This occurs under the rare condition when controllers are present in a redundancy environment with a active and standby controller, and simple IP sessions are opened. Tracebacks may appear on the backup controller after sessions are opened.
Workaround: none.
- CSCed86177—Tracebacks Found on PDSN (ip_feature_fastswitch) (Clustering)
A Cisco router running 12.3T R2.0 Release PDSN software sometimes produces tracebacks while sending bidirectional traffic from mobile node to reflector in SIP flow with compress stack enabled and CEF switched
The condition occurs when sending bidirectional traffic from mobile node to reflector in SIP flow with compress stack enabled, and CEF switched tracebacks can be seen on PDSN console.
Workaround: none.
- CSCin78876—MIP CPS Low With Mobile IP Global Configuration
A Cisco router running PDSN 2.0 Release software (Cisco IOS 12.3T) has a lower CPS rate for Mobile IP calls
The number of MIP calls that can be established per second is below 30.
Workaround: none.

Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.3(14)YX13:

- CSCso89250—Gigawords Attributes Not Sent During IS835b Handoff
Acct-Input-Gigawords and Acct-Output-Gigawords are not sent during handoff.
This condition occurs if the handoff performed is IS-835B.
Workaround: perform IS-835a handoff by configuring the **cdma pdsn compliance is835a handoff** command.
- CSCsq70473—MWAM RX Driver Halts Under Heavy Traffic
The MWAM processor gigabit ethernet interface stops processing traffic.
This condition occurs at a high rate of incoming traffic.
Workaround: restarting the interface (shut/no shut) will restore the traffic forwarding.

Resolved Caveats Prior to 12.3(14)YX13

The following caveats are resolved in Cisco IOS Release 12.3(14)YX12:

- CSCei00766—Router Crash With LCP Packet Loop
A router may crash when the encapsulation is set to PPP and repeatedly removed.
This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3 or Release 12.4 and that is configured for PPP Link Control Protocol (LCP).
Workaround: none.
- CSCso81854
Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.
To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.
Cisco has released free software updates that address these vulnerabilities.
This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml>.
This security advisory is being published simultaneously with announcements from other affected organizations.

Resolved Caveats Prior to 12.3(14)YX12

The following caveats are resolved in Cisco IOS Release 12.3(14)YX11:

- CSCsh79103—Newly Added Member PDSN Reloads Under Stress Conditions

On a Cisco router running Cisco IOS Release 12.3(14)YX5 software, a newly added member PDSN reloads under stress conditions.

This condition occurs when a member PDSN is separated from the cluster using the **cdma pdsn cluster member prohibit administratively** command, the member interface is unconfigured using the **cdma pdsn cluster member interface** command while sessions are still present, and then the member PDSN is added back to the cluster and the member interface is reconfigured.

Workaround: When removing a member PDSN from a cluster, change the necessary configuration, save the configuration, and reload the router.
- CSCsk36647—Accounting Start Missing if Dormant Handoff is Followed by an Active Start

An Accounting Start record is sent when there are update values received, followed by an Accounting Stop record, which is sent for the start initiated by the connection setup.

This condition occurs when an Accounting Start is received during dormant handoff.

Workaround: Configure the **cdma pdsn accounting send start-stop** global configuration command.
- CSCsk72404—PDSN Cluster Controller Reloads on Chunk Corruption

On Cisco router running Cisco IOS Release 12.3(14)YX10 software, a crash is observed due to chunk corruption that is caused by session list handling of MN records.

This condition is observed when International Mobile Subscriber IDs (IMSI) 10 or 11 digits long exist in the network, and they are prefixed with zeros.

Workaround: none.
- CSCsk73104

Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

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

Resolved Caveats Prior to 12.3(14)YX11

The following caveats are resolved in Cisco IOS Release 12.3(14)YX10:

- CSCsj10784—Spurious Access Seen During MSID Calls During Deregistration

On Cisco router running 12.3(14)YX4 software, spurious access occurs on MSID Calls during Deregistration.

When a MN terminates an MSID call before an authentication response is received, if the authentication response is received on termination of PPP with A10 still up, spurious access is observed.

Workaround: none.

- **CSCsj12489—Memory Corruption in OpenRP to ClosedRP Handoff Scenario**
Memory corruption occurs when a user handoff is from ClosedRP PCF to OpenRP PCF.
This occurs on a Cisco router running 12.3(14)YX04 PDSN software on an MWAM card. Memory corruption is seen for a IS-835a handoff from ClosedRP PCF to OpenRP PCF.
Workaround: none.
- **CSCsj16007—PDSN Reloads at aaa_db_add_data**
The PDSN member reloaded at find_elt.
This occurs on a PDSN using IOS version 12.3(14)YX8.
Workaround: none.
- **CSCsj25133—Unable to Open More Than 50k Sessions with Random IMSI**
On a Cisco router running PDSN release 12.3(14)YX4, cluster controller is only able to handle 50k EVDO (random IMSI) sessions.
This occurs only with PCFs changing the IMSI to a random IMSI. For the 1xRTT with incremental IMSI, no issues are seen.
Workaround: none.
- **CSCsj34462—Bad Refcount Errors in AHDLC Decode**
Bad refcount error messages are seen on a Cisco router running PDSN 12.3(14)YX4 software.
This condition occurs when doing a AHDLC decode in interrupt path (packet less than 30 bytes) and packet is not a good packet (FCS errors or invalid datagram).
Workaround: none.

Resolved Caveats Prior to 12.3(14)YX10

The following caveats are resolved in Cisco IOS Release 12.3(14)YX9:

- **CSCsa86289—Router Hangs During NBAR Classification**
A 2811 router hang every 3-4 days.
The router is running 12.3(14)T and NAT, PPPoE and DNS proxy are configured on the router.
Workaround : none.
- **CSCsi40241—Cluster Member Displayed Twice in the Controller**
In the 3.0 YX6 release, we found duplicate member entry while removing one of the members from the cluster. This is visible only on the standby controller.
Workaround: none.

Resolved Caveats Prior to 12.3Y(14)YX9

The following caveats are resolved in Cisco IOS Release 12.3(14)YX8:

- CSCse32483—PDSN Reloads on High Mobile to Mobile Traffic

Device may experience a bus error or a Stack low for Level 1 interrupt.

When there is a mobile to mobile communication, both decoding and encoding happens in the same code flow. In the event of high mobile to mobile traffic, this can lead to stack overflow in both the interrupt path and process paths.

This condition occurs on all PDSNs with high mobile to mobile traffic.

Workaround: none.
- CSCse89861—No Authentication for Domain in LAC

L2tp does not start for users authenticated using radius although “Service-Outbound” is returned as well as VPDN avp-pairs.

This condition occurs when trying to bring the VPDN with Radius authentication on 12.3(14)YX2

Workaround: none.
- CSCsf16294—Same NAI, Different IMSI / HA - PDSN Should Trigger a Revocation to Old HA

On a Cisco router running Release 3.0 PDSN software, when the MN connects with the same NAI (but a different IMSI) to a different HA (HA1 and HA2), and the **ip mobile cdma imsi dynamic** command is configured, the PDSN does not send any revocation message to delete the binding on HA1. As a result, HA1 has a stale binding entry.

This condition only occurs when the same user connects with a different IMSI to a different HA.

Workaround: none.
- CSCsg05312—Remove ACFC for Downstream VPN Traffic in PDSN

On Cisco router running Release 3.0 PDSN software, for a VPDN call, the ACFC (0xFF03) is present in the downstream VPN traffic towards mobile node, even though ACFC has been negotiated. This causes certain mobile node types to drop these packets.

This only occurs for downstream VPN traffic while ACFC has been negotiated.

Workaround: none.
- CSCsg33992 Memleak Seen During PPP Renegotiation Using Sub-interfaces

There is a memory leak of 64 bytes per session seen during PPP renegotiation and handoff.

This condition occurs on all PDSN images with sessions created using subinterfaces. On the YF image, TCP header compression created full interfaces, but on the YX images only subinterfaces are created.

Workaround: Configure the **ip irdp** command on the Virtual-Template.

To send MIP advertisements, 3 Multicast addresses (ALLSYSTEMS, ALLROUTERS and ALLMIPROUTERS) are attached to a queue and associated with the interface.

Whenever a renegotiation happens, ALLMIPROUTERS is freed and then the queue is reinitialized thereby leaking the ALLROUTERS and ALLSYSTEMS memory.

- CSCsg67390 —F5 is Not Getting Updated After Making Session Active

On a Cisco router running the Cisco 12.3(14)YX4 PDSN software, the Service-Option value is not updated when a session becomes active after a dormant handoff.

This issue occurs under the following conditions:

- When the **cdma pdsn accounting send start-stop** command is not configured in PDSN.
- The MN is dormant in PcfA, and does a dormant handoff to PcfB.
- The MN is now made active in PcfB, and an active start is sent to PDSN. Here the active start sent from the PcfB is not updated on the PDSN.

Workaround: if you configure the **cdma pdsn accounting send start-stop** command, this issue will not be seen.

- CSCsg94481—PDSN Stats Per pcf by SNMP Query Shows the Same Value

PDSN Stats per pcf by an SNMP query shows the same value.

CISCO-SMI::ciscoMgmt.157.1.7.10.1.1.24.1.4.8.8.8.0 = Gauge32: 47

CISCO-SMI::ciscoMgmt.157.1.7.10.1.1.24.1.4.9.9.9.33 = Gauge32: 47

This symptom occurs on a Cisco 12.3(14)YX2 PDSN image. The problem happens when query .1.3.6.1.4.1.9.9.157.1.7.10.1.1

Workaround: none.

Resolved Caveats Prior to 12.3Y(14)YX8

The following caveats are resolved in Cisco IOS Release 12.3(14)YX4:

- CSCir00110 —AAA Low Memory Thresholds

AAA Low Memory Threshold Feature provides a user configurable mechanism, for handling low memory conditions.

For porting this feature into the YX3 throttle, we need to port the following ddtss,

CSCef29940

CSCsd27777

CSCin99788

CSCei26961

- CSCir00712—LAC Does not Handle Process Switched Packets- Fragmented Data Traffic

On a Cisco LAC software running IOS version 12.3(14)T, when the fragmented data traffic is received on the LAC over the L2TP tunnel, instead of consuming the L2TP data traffic locally, the IP layer reassembles the packet and routes the packet on the wrong interface.

This condition exists when fragmented L2TP data traffic is received on the LAC from the LNS over the L2TP tunnel.

Workaround: none.

- CSCsb30480—Out-of-Sequence Acct-Response Packets triggers Interim Accounting

On a Cisco router running R2.1 PDSN software, after a dormant handoff, the PDSN periodically sends “Watchdog” packets to the RADIUS server where the Accounting-Response received from the RADIUS server are “Out of Sequence”.

This issue occurs during a dormant handoff only if the “Accounting-Reponse” for the Accounting-Stop is received first, then followed by Accounting-Response for the Accounting-Start.

Workaround: none.
- CSCsd46212—SNMP Query for cCdmaHDLCogRESessionTotal Does Not Return Any Value

The SNMP query for the Mib object cCdmaHDLCogRESessionTotal does not return any value. Since this mib object does not return any value in NMS applications like Ciscoview, this object throws an error as no value in returns from SNMP agent.

Workaround: none.
- CSCse29358—Service-Option (F5) is set to 0 in Acct-Stop during handoff.

On a Cisco router running 12.4(7.9.1)PIL5 software, the Service-Option value is set to 0 in an Acct-Stop message during dormant / Active handoff.

This issue occurs only when a dormant / active handoff is triggered

Workaround: none.
- CSCse39034—IO memory Depletion with Slow RADIUS Server Responses

An MWAM card running version 2.1 of the PDSN software can experience low IOMEM conditions. When this occurs, it may not be possible to session to the processor consoles. Tracebacks relating to IO Memory allocation failure may also be seen.

This condition occurs when the load on the RADIUS server used for authentication and accounting is high, and there are a large number of RADIUS timeouts and subsequent re-transmissions.

Workaround: ensure that the number of RADIUS timeouts and re-transmissions is not excessive.
- CSCse63330—MWAM/PDSN - MIP RRP Does Not Contain New Challenge For Re-registration

When using the simulator image to generate a MIP call to a Cisco PDSN running the R2.1 12.3(11)YF3 image, the PDSN does not send a new MN-FA challenge in RRP for a MN to use on its next attempt at re-registration.

In the situation where the previous RRQ failed (due to code 136—unknown HA address), RRP does not contain any challenge extension (let alone new extension for next registration). This behaviour results in a “stale challenge error condition”, where the re-registration continuously uses the first challenge extension that gave us error code 136.

Workaround: none.
- CSCse71921—Release Indicator nOt Sent While Doing Active-handoff After Switchover

On a Cisco router running IOS 12.3(14)YX3 software, the F13 “Release Indicator” is not sent in an Accounting Stop message for the old PCF. This happens while doing an active-handoff after a switchover.

This condition occurs in session redundancy mode, after doing switchover.

Workaround: none.

- CSCse71950—Reusing of Acct-Session-Id After Doing Dormant Handoff

On a Cisco router running Cisco IOS 12.3(14)YX3 software, after fresh bootup of the PDSN, the PDSN reuses the Acct-session-id for the very first user who undergoes a dormant or active handoff.

For subsequent handoffs this issue is not seen.

This issue occurs under the following conditions:

- With and without the **cdma pdsn accounting send start-stop** command configured on PDSN.
- On standalone and redundant PDSN setups.

Workaround: none.

- CSCse71974—Multiple Acct Msgs Sent When Airlink Active Start Message Received

On a Cisco router running Cisco IOS 12.3(14)YX3 software, after doing dormant handoff, if we send an airlink active start, the PDSN sends three Accounting packets instead of a single accounting start packet.

This issue occurs whether the **cdma pdsn accounting send start-stop** command is configured on the PDSN, or not.

Workaround: none

- CSCse72317—Duplicate Correlation Ids from PDSN

On a Cisco router that is running Cisco PDSN software, duplicate correlation IDs are seen.

This condition occurs when the user (NAI) connects with different MN identities (IMSI/MIN) using different HAs.

In situations where there is already an existing MN session, if the same user (same NAI in Mobile IP RRQ) connects with a different MN identity and HA address, the correlation ID for the session is being reused.

Workaround: none.

- CSCse80960—Radius Session-timeout '0' Fails to set MIP Absolute Timeout to Infinite

During the second phase authentication (realm based) of a MIP call, a radius session-timeout of 0 fails to remove the the absolute timeout in the output of the **show int virtual-access** command. The absolute-timer configured on the Virtual-Template is maintained.

- CSCse92943—PDSN reloads When the Same NAI Connects with Different IMSI

On a Cisco router running R3.0 PDSN YX3 Software, PDSN reloads consistently in the scenario where the same NAI connects with Diff IMSI (EVDO cases) and when the MIP re-registration happens through the newly connected PCF.

The reload occurs only when the same user (NAI) is connected with a different IMSI (EVDO). This can happen in two different scenarios depending on whether the **ip mobile cdma imsi dynamic** command is enabled or not.

- Without **ip mobile cdma imsi dynamic** configured: when MN re-registers with the new IMSI to the same HA, PDSN reloads.
- With **ip mobile cdma imsi dynamic** configured: the MN may download a different HA (using dynamic HA assignment) whenever it authenticates. In this scenario, when MN re-registers with the new IMSI and a different HA, PDSN reloads.

Workaround: for a single HA scenario (MN always registers to same HA), the **ip mobile cdma imsi dynamic** command can be configured to work around this.

For scenarios where MN gets a different HA whenever it authenticates using new IMSI, there is no known workaround.

- CSCsg06628—Session Timeout is not Applied to Mip Flows
On a Cisco router running Cisco IOS 12.3(14)YX4 software, the session timeout value configured on virtual-template is not applied to the MIP flows. Additionally, this occurs in SIP, if the authentication is performed using AAA rather than the local.
This condition occurs when you manually configured the session timeout on the virtual-template
Workaround: none.

Resolved Caveats Prior to 12.3Y(14)YX4

The following caveats are resolved in Cisco IOS Release 12.3(14)YX3:

- CSCsa60842—Precloned Vaccess Interfaces Stuck in Status 0x84 and not Reused.
When a Cisco 7200 router running IOS 12.3(12a) is configured to aggregate PPPoE sessions and the **virtual-template x pre-clone y** command is used to pre-clone Virtual-Access interfaces, the pre-cloned Virtual-Access interface may become unusable after a user disconnects.
The virtual-access interface will be down/down and have a Vaccess status 0x84, free pending PPP completion when the show interface virtual-access command is used.
New connection attempts will not be able to use the affected virtual-access interfaces which also may cause new virtual-access interfaces or subinterfaces to be cloned.
If the **show template** command is issued the “Current Free Pending” counter will indicate the number of Virtual-Access interfaces that are currently in this state.
The conditions that cause this problem to occur are currently not known. The problem does not occur every time a user disconnects and frees a virtual-access interface.
Workaround: currently there is not a workaround for this problem except to not pre-clone virtual-access interface by removing the **virtual-template x pre-clone y** command.
- CSCsd20371—Router Crash by Race Between Displaying And Removing Conditional Debugs
Displaying conditional debugs with the **show debug condition** command on the console port, and removing this condition from vty port simultaneously causes the router to crash.
The crash occurs only when these two actions are executed at same time.
Workaround: avoid executing these two actions simultaneously.
- CSCse30454—Bus Error at swsb_link
Device may experience a bus error.
There are no known conditions that cause this symptom to occur.
Workaround: none.
- CSCse34167—PDSN Reloads When **no debug** Condition All Executed
PDSN might reload after issuing the **no debug condition all** command.
Workaround: none.
- CSCse35947—**show module** on Supervisor Does Not Display the Correct AP Version
The **show module** command on the supervisor still shows the older version, even though the other places have been correctly updated.
Workaround: none.

- CSCin99755—Acct-Session-Time sent in ACCT STOP Mesg in PDSN is Incorrect

A Cisco router running PDSN software sends an incorrect value for Acct-Session-Time in accounting Stop Messages. This may lead to overcharging.

The over charging happens when Acct-Session-Time is used for charging the user.

This condition occurs only if there are any interim acct start-stop messages (caused due to change in airlink parameters or handoff) sent for the session.

When Acct-Session-Time is used for charging, PDSN will not reset the value after sending the interim acct stop messages. This results in overcharging.

Workaround: G8 can be used for charging.

Resolved Caveats Prior to 12.3Y(14)YX3

The following caveats are resolved in Cisco IOS Release 12.3(14)YX2:

- CSCin99350—PPP Counters Wrongly Increment In case Of Simple IP to VPDN Users

For a Cisco router running 12.3(14)YX1 PDSN software, global statistics, **show cdma pdsn stat ppp** can encounter a mismatch such as, requests less than sum of success, failure and aborted.

This condition occurs in the presence of certain kind of mobile, that connects as simple ip users, and then re-negotiates ppp as vpdn users.

Workaround: none.

- CSCsd78129—PDSN Memory Leak at PPP Related Process

On a Cisco router running version 2.1 of the PDSN software, processor memory held by the PPP Bind, PPP Events and PPP Hooks processes may increase continuously.

This condition only occurs when VPDN sessions are terminated by the PDSN due to idle timeout.

Workaround: do not configure an idle timeout for the VPDN sessions in PDSN.

- CSCsd79249—PPP fAilure Connection Counters Mismatch for PDSN Release 3.0

On a Cisco router running 12.3(14)YX1 PDSN software, during execution of the **show cdma pdsn stat ppp** command, a failure reason counter mismatch between total and subcounter is observed.

“Failure reason - Other” counter was not incrementing, and remain at 0.

This is a normal operation.

Workaround: none.

- CSCsd84703—**ip mobile cdma ...** CLI Chain Broken

On a Cisco router running the 12.3(14)YX1 PDSN software, the **ip mobile cdma ...** CLI chain option is not supported.

Workaround: none.

Resolved Caveats Prior to 12.3Y(14)YX2

The following caveats are resolved in Cisco IOS Release 12.3(14)YX1:

- CSCsc87480 [MEID]—PDSN Reloads When a MIP Flow is Opened With/Without MEID in RRQ
A PDSN with MEID support reloads when a mip flow is opened with or without MEID in the RRQ. The issue occurs when **no service alignment detection** is configured on the PDSN.
Workaround: do not configure **no service alignment detection** on the PDSN.
- CSCsc74745—PDSN Deletes Old PCF Details When PPP Negotiation Starts During Handoff
If the PPP re-negotiation starts for the mobile during the handoff, the PDSN deletes the old PCF details.
Workaround: enable the **cdma pdsn compliance is835a handoff** command on the PDSN.
- CSCin97926—PDSN **show ppp stats** - Failures, Reneg, Term Req In LCP Inconsistency
On Cisco router running the PDSN software, the counters in the **show cdma pdsn statistic ppp** command do not increment as expected.
This occurs under normal conditions.
Workaround: none.
- CSCsc71683—Accounting-Gigawords Not Present in PDSN Accounting Records
When the uplink or downlink data transfer volume for a PDSN call exceeds 4 Gigabytes (2^{32} bytes), Acct-Input-Gigawords or Acct-Output-Gigawords attributes should be included in RADIUS Accounting requests. However, these attributes may not be present.
In addition, input and output byte counters in the **show interface Virtual-Access** command may simply roll over to 0. Counters seen in the **show cdma pdsn accounting** command, on the other hand, will show correct values.
This issue occurs in a PDSN configuration using IOS 12.3(11)YF.
Workaround: none.
- CSCsc69520—F13 Not Sent in Accounting Stop Record When a Dormant Session Tears Down
On Cisco router running 12.3(14)YX PDSN software, the F13 attribute is not sent in an accounting stop when a dormant session is made to tear down.
The F13 attribute is not sent in accounting stop only when the session is closed during dormant state. If you tear down the session while it is in active state, no issues occurred.
Workaround: none.
- CSCsc90240—Sessions Created After Peer Loss Not Bulk Synced After Peer UP
Sessions created during an active-active scenario do not get synced up after its recovery.
This condition occurs whenever link failure in an HSRP group happens, and a call is made through the PDSN that takes the active role.
Workaround: none.

- **CSCin98817—PDSN MWAM Bus Error During Deletion of PPP Conditional Debug**
 A PDSN running the 12.3(11)YF2 based engineering special is reloaded due to bus error.
 A reload occurs while deleting the PPP conditional debug. This is a rare event, as the bus error occurs only when the deletion of PPP conditional debug happens simultaneously with the connection deletion.
Workaround: none.
- **CSCsd50241—EXTRA TRAILING 0x00 in Calling Station ID When Setting Up L2TP from PDSN**
 On a Cisco PDSN, when mobile nodes open a VPDN service type flow, the PDSN sends a ICRQ message to LNS. In this message the PDSN includes the MSID of the mobile. When the Calling Station (MSID) AVP is added, the PDSN adds an extra “0x00” character at the end of MSID. This may cause the ICRQ to be rejected on the LNS, since the length field in the Calling Station AVP does not include the extra character.
 This condition occurs whenever VPDN service type is provided to the mobiles on the PDSN.
Workaround: none.
- **CSCsd03974—Standby PDSN Stores Incorrect MEID Value in UDR**
 The standby PDSN stores an incorrect MEID value in UDR.
 This condition occurs when a different MEID value is received in setup and stop records with PDSN redundancy enabled.
Workaround: ensure that PCF does not send different MEID values in airlink records when PDSN redundancy is enabled.
- **CSCsc46303—MIB Sanity Check RP Update and ACK Counters Do Not Match**
 On a Cisco router running the Cisco IOS 12.3(14)YX PDSN image, “CdmaRpUpdTransmittedReqs” counter values do not match with the sum of “CdmaRpUpdateAccepted”, “CdmaRpUpdateDenied” and “CdmaRpUpdateNotAked” counters.
 This condition may be the result of a race condition on the PDSN.
Workaround: none.
- **CSCin97998—PPP Conn Req Mismatch With Success+Failure+Aborted**
 In the PDSN 3.0 EFT Image, the **show cdma pdsn stat ppp** command shows inconsistent counter values when IPV4 and IPV4 stack co-exist.
 This condition occurs when the **cdma pdsn ipv6** command is configured.
Workaround: do not configure the **cdma pdsn ipv6** command.

Caveats Resolved Prior to Cisco IOS Release 12.3(14)YX1

The following caveats are resolved in Cisco IOS Release 12.3(14)YX:

- **CSCin86674—PPP Connection Aborted Counter Increments with WRONG MSID Session**
 On a Cisco router running R2.0 Home Agent software, PPP connection Status (Connection Aborted counter) increments on creating Simple IP Session with Incorrect MSID value.
Workaround: none.

- CSCeh41261—Connection Aborted Counter Increments During auth Timeout
On a Cisco router running the PDSN image, the connection aborted counter is incrementing instead of failure counter during auth timeout.
Workaround: none.
- CSCin97444—Current Connections Decrement For Wrong SO in per-PCF PPP Stats
On a Cisco router running PDSN Cisco IOS Release 12.3(11) software, counters displayed by **show cdma pdsn statistics ppp pcf** are not correct.
This issue occurs during handoff.
Workaround: none.
- CSCin97765—Connection Req in PDSN ppp pcf stat is Abnormal
On a Cisco router running PDSN Cisco IOS Release 12.3(11) software, it is observed that the connection req field in **show cdma pdsn stat ppp pcf** is an unreasonably large value.
Workaround: none.
- CSCin88503—PDSN Crashed During Handoff
A Cisco PDSN running the 12.3(11)YF image may reload while handoff of a session happens from one PCF to another.
This is a rare scenario during the inter-pcf handoff.
Workaround: Configure the **cdma pdsn compliance is835a handoff** command.
- CSCsa79410—PDSN MIP Client Upload Fails With Large IP Packet
On a Cisco router running PDSN IOS Release 12.3(11) software, when uploading files from a Mobile IP client to a server through the PDSN, packets that are larger than 1480 bytes and the DF bit is set are dropped by the PDSN. The PDSN does not send ICMP UNFRAG error to MIP client, therefore it fails to learn the smaller mtu path. The mip client will continue to send packets larger than 1480, and it will never get to the server. SIP clients are not affected.
The IP MTU setting for the IP/IP tunnel between the FA and HA is 1480 bytes.
Workaround: configure **no ip mobile tunnel path-mtu-discovery** to disable path MTU discovery on the PDSN.
- CSCsb11124
The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.
Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.
Cisco has published a Security Advisory on this issue; it is available at <http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>
- CSCsb39828—PDSN Sends Packets out of Sequence When MPPC Compression is Enabled
On a Cisco router running PDSN IOS Release 12.3(11) software, it is found that the PDSN is sending MPPC compressed packets out of sequence towards client.
This issue occurs only when MPPC is enabled.
Workaround: none.

- CSCsc03364—MWAM - Bus error in 12.3(11)YF3
A Cisco 7609-MWAM Router running the “svcmwam-c6is-mz.123-11.YF3” image reloaded due to a Bus Error at invalid address. This occurs because of a race condition that the session gets deleted while receiving traffic. This is a rare scenario.
Workaround: none.

Caveats Resolved Prior to Cisco IOS Release 12.3(14)YX

The following caveats are resolved in Cisco IOS Release 12.3(11)YF4:

- CSCei61732
Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.
Cisco has made free software available that includes the additional integrity checks for affected customers.
This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.
- CSCei76358—os-boot Cleanup of User Interface Data
Through normal software maintenance processes, Cisco is removing deprecated functionality from the OS boot routine. These changes have no impact on system operation or feature availability.

Caveats Resolved Prior to Cisco IOS Release 12.3(11)YF3

The following caveats are resolved in Cisco IOS Release 12.3(11)YF3 and are listed by component:

PDSN

- CSCef39342—Non-Crypto Packets Dropped Due to CDMA and CLI IPSEC Interoperability
When CDMA IPsec is configured on the PDSN and CLI IPsec is configured on the HA, in the absence of a IPsec user MIP tunnel, normal IP traffic is dropped because no crypto tunnel is established between PDSN and HA.
This symptom has been observed on the PDSN and HA routers running Cisco IOS release 12.3T.
Workaround: none.
- CSCef75738—PDSN Rejects an RRQ With Active Stop If Prior Record Not Start/stop
Rp counters are not incrementing in a Cisco router running 12.3T R2.0 Release PDSN software. The PDSN rejects an RRQ with Active Stop if a prior record is not started or stopped.
Workaround: none.

- CSCin88336—CISCO-ENHANCED-MEMORY-POOL Objects are not Populated in R2.1
CISCO-ENHANCED-MEMORY-POOL objects are not populated in Release 2.1
No specific condition. This happens when the objects of this MIB is queried.
Workaround: none.
- CSCin89969—PDSN Deletes Session Incorrectly Due to MobileIP RRQ Timeout
On a Cisco PDSN the simple IP flow is deleted incorrectly due to mobile ip registration request timeout. The race condition for deleting the session incorrectly only if all the following condition matches
Mobile Node in the initial PPP negotiation rejects PPP Authentication and during the IPCP stage does not include the IP Address options in the IPCP ConfReq.
Mobile Node before the initial Mobile IP registration request (cdma pdsn timeout mobile-ip-registration) timeout occurs, does PPP renegotiation. During the PPP renegotiation the mobile request for PPP authentication and includes IP address options in the IPCP stage because of which Simple IP flow is created.
Workaround: none. The mobile needs to be configured to do PPP authentication.
- CSCin91064—PPP Packets over PPPoGRE Session Dropped for VPDN Flows
On Cisco router running R2.1 PDSN software, the PPPoGRE session is dropped for VPDN flows if PPP-acfc packet is received with FF03.
This issue is seen only for VPDN session and for SIP.
Workaround: none.
- CSCin91735—AHDLC IO Memory Leak for BadCRC packets with no ahdlc trailer closed rp
On Cisco PDSN software running 12.3(11)YF1 image with Closed RP feature enabled and the **no cdma pdsn a10 ahdlc trailer** command is configured. If AHDLC packets with Bad CRC errors are received then IO memory allocated for the packets are not released which may leads to low IO memory situation on the PDSN.
Workaround: configure the **cdma pdsn a10 ahdlc trailer** CLI.
- CSCin92305—Dormant Handoff Triggers Interim Accounting
After dormant handoff, with **cdma pdsn accounting send start-stop** configured, the PDSN starts sending out interim accounting records to the RADIUS server.
In IOS, RADIUS watchdog records are not triggered after an accounting STOP is sent to the RADIUS server. They are only sent after an accounting START is sent. However, it is observed that after dormant handoff, with **cdma pdsn accounting send start-stop** configured, the PDSN starts sending out interim accounting records to the AAA server. This is not expected, as an accounting STOP is sent to the AAA server during the dormant handoff process.
In the case of dormant handoffs with **cdma pdsn accounting send start-stop** configured, the following is observed:

 - a. When a simple IP session is opened, an Accounting START is sent (as expected) with e.g. Accounting Session ID = 1.
 - b. Watchdog records are sent at the configured interval.
 - c. When the session is made dormant, an Accounting STOP is sent (as expected) with eg. Accounting Session ID = 1.

Now, when a dormant handoff is executed:

- a. The target PCF sends an airlink SETUP. The PDSN then sends an accounting START followed by an accounting STOP (as expected) with e.g. Accounting Session ID = 2.
- b. When the source PCF sends a Reg Upd Ack, the PDSN then again sends an accounting START followed by an accounting STOP (as expected) with e.g. Accounting Session ID = 3.
- c. After the above sequence, it is found that the PDSN incorrectly sends watchdog records with Accounting Session ID = 2. These records should not be sent, as a accounting STOP has been sent.

Workaround: none.

- CSCin92122—Abort Does Not Increment in **show cdma pdsn stat ppp pcf**
Statistics counter corresponding to Abort in **show cdma pdsn statistics ppp pcf** does not increment. This condition occurs on a Cisco router configured for PDSN.

Workaround: none.

- CSCin92700—Incorrect Downstream Accounting With TCP Header Compression Enabled
On Cisco Packet Data Service Node(PDSN) when TCP header compression is enabled and mobile negotiates TCP header compression, then incorrect accounting is done on the packet bytes by the PDSN for the downstream direction.

Workaround: none.

- CSCsa67420—PDSN: Spurious Access and Bus Error Crash in PPP Compression
A 7200 PDSN running 12.3(4)T and configured for MPPC might crash by Bus error. Right before the reload, the following Alignment Error is displayed:

```
%ALIGN-1-FATAL: Illegal access to a low address
```

This condition occurs on a PDSN running IOS version 12.3(4)T or later, that is configured for MPPC.

Workaround: none.

CSCsa93388—PDSN Not Parsing SDB if g10 Sent Before Y4 With ios4.1 Compliance

On Cisco router running PDSN software, the PDSN throws parsing error if g10 attribute received before y4 in the SDB record.

The PDSN should be able to parse the SDB records in whatever order the data arrives.

This issue occurs in PDSN YF release images, and also when ios4.1 compliance for SDB record is enabled.

Workaround: none.

MWAM

- CSCeh67507—MWAM Processor Hangs, SR system Unavailable When Lot of Debugs Enabled
MWAM processor appears to be hung. However it does send out HSRP hellos now and then causing its peer to not takeover or cause RF induced reloads on peer (based on HSRP priority). So, SR system does not recover completely. Note that this affects the partner processors in the same complex as well.

This condition occurs when too many debug or error messages are printed.

Workaround: configure **no logging console guaranteed** to avoid lock up of the console, or the logger process hijacking the CPU.

NAT

- CSCef50065—NAT Causes Spurious Memory Access Made at 0x80A3B064 Reading 0x36

Spurious memory accesses and tracebacks are generated on a Cisco 831. This symptom is observed when NAT/PAT is configured.

Workaround: none.
- CSCef97573—NAT: H225/H245 pak Cause Crash in ipnat_destroy_seqdelta

A router may reload with a bus error exception, the crashinfo file shows an address error (a load or instruction fetch), and there is a spurious access in the crashinfo file. These symptoms are observed on a Cisco router that performs NAT on H.323 voice traffic.

Workaround: none.
- CSCsb22290—NAT Overload Broken With CLI **ip nat service fullrange udp port 500**

When the user configures the **ip nat service fullrange udp port *number*** command, the port-allocation logic is broken. If a PAT port is taken the next-port logic fails.

The **ip nat service fullrange** CLI is only for specific customers, and the regular port-allocation logic is not affected. Only when this command is enabled are things broken as explained above.

Workaround: disable the **ip nat service fullrange** CLI if it is enabled.

Miscellaneous

- CSCee45312—Radius Authentication Bypass When Configured With a None Fallback Method

Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

More details can be found in the security advisory which posted at the following URL <http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml>
- CSCef73460—ISA Card Not Detected in C7200 Router

An ISA encryption card is not activated when you boot the router.

This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(11)T or interim Release 12.3(11.4) and that is configured with an NPE-400. Note that the symptom does not occur when the router is configured with an NPE-G1.

Workaround: none.

Caveats Resolved Prior to Cisco IOS Release 12.3(11)YF3

The following caveats are resolved in Cisco IOS Release 12.3(11)YF3:

- CSCef97018—VAM2: Authentication Error and Invalid packet Errors at High Stress

A Cisco 7200 router with VAM2 will display many output authentication errors and invalid packet errors.

This condition occurs under high stress and when QOS pre-classify is configured.

Workaround: Disable QOS or reduce the traffic rate.

- CSCeg08326—MWAM: Mobile IP Tunnel Source and Destination Reported as UNKNOWN

A Cisco Home Agent router may report the tunnel source and destination, for a dynamically created Mobile IP-IP Tunnel, as “UNKNOWN” in the **show interface** command output.

```
Router# show interface t1
Tunnell1 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of Ethernet0/0 (10.1.1.1)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source UNKNOWN, destination UNKNOWN
```

Workaround: none.

- CSCeg17877—Common Crypto Engine Pak Cleanup

This DDTS is not a bug. The diffs for this DDTS provide functionality that is utilized by the fix for bug CSCeh14272.

Since CSCeh14272 needs to go into a throttle, CSCeg17877 will also need to go into a throttle.

(The commit moves duplicate functionality out of a pair of drivers into the common code for help with maintainability.)

- CSCeh23419—PDSN R2.0: acct-stop Wrong Release ReasonID

This behavior is seen when a timeout value is configured on the PDSN for a PPP session, and the PCF terminates the session. Since the timeout value is configured for the session, the PDSN does not respond to the LCP term req until the timeout value. If a RRQ with lifetime zero is received for the session, the PDSN terminates the session immediately and removes the timer. In this scenario, the `cdma_release_ind`, which is one of the 3gpp2 radius attributes, was not set properly. Ideally this needs to be set to “PPP Termination”.

This condition occurs when RRQ 0 is received before the timeout expiry in the PDSN for session termination.

Workaround: none.

- CSCin46180—PDSN Should Not Reject Retransmit Sequence Number in A11 RRQ with 2 Airlink Received

The Cisco Packet Data Serving Node(PDSN) running 12.2(08)ZB01 image may reject registration request (RRQ) received on the Packet control function (PCF) and PDSN signalling interface(A11) by setting reply code to 8DH in the A11 registration reply (RRP)sent back to PCF.

This condition exists when an A11 RRQ with two airlink records (setup airlink record and start airlink record) is retransmitted, and the airlink sequence numbers in the airlink records is same as received in the previous A11 RRQ.

Workaround: none.

- CSCin81520—Extra Mobile IP Debugs are Printed for Conditional Debugging
Some extra mobile IP debugs are printed on Cisco PDSN running 12.3(08)XW software when mobile IP conditional debugging is enabled on it. Debugs that get printed are not corresponding to the user.
Workaround: none.
- CSCin86716—PDSN to Parse SDB Records as Per IOS 4.x
The Cisco PDSN cannot parse A11 Registration request message from PCF that contains attribute value 32 in SDB airlink record.
This conditions exists when the PCF sends attribute value 32 in SDB airlink record.
Workaround: none.
- CSCin86601—PDSN a11 session update retransmission is not working correctly
The Cisco PDSN is not taking the configured a11 session update timeout value into consideration while retransmitting the a11 session update message.
This condition occurs when the Cisco router is configured for the PDSN.
Workaround: none.
- CSCin86667—SDB Airlink Record Rejected After Dormant Handoff
When an SDB airlink record is received after a SETUP/START airlink record, the RRQ is rejected with an error code of 86H, with the following debug printed:
 “Bad Airlink record. Received SDB airlink after SETUP/START”.
Workaround: None.
- CSCin86686—Interim Accounting Behavior Changed for Dormant-Active Transition
In the following PDSN scenario, the interim accounting update interval is not working properly.
This problem occurs when the following conditions exist:
 - a. Open a call.
 - b. Force the call to dormant state.
 - c. Wait for less than PPP idle timeout value.
 - d. Force the call to active state.**Workaround:** none.

- CSCin88505—Active and Dormant Session Counts Incorrect After Handoff

The Active Session Counter and Dormant Session Counter carry junk values upon handoffs. The junk values are observed in the following scenarios:

Scenario 1:

- Open a Simple IP flow with PCF1 --- Keep the session Active
- Handoff the flow to PCF2
- Active Count becomes 2 and Dormant Count Becomes Junk Huge Value.

Scenario 2:

- Open a simple IP flow with PCF1 (keep session active).
- Make the session dormant.
- Handoff the session to PCF2.
- Make the session dormant.
- Active count carries a huge junk value.

Workaround: none.

- CSCsa46707—VAM2 Encryption Card Stops Encrypt/Decrypt Traffic After a Few Hours

An SA-VAM2 stops processing all packets.

This condition is observed sporadically on a Cisco 7200 series that is configured with an NPE-G1 when the SA-VAM2 is configured for AES 192 or AES 256.

Workaround: Reset the SA-VAM2 by entering the **no crypto engine accelerator** command followed by **crypto engine accelerator** command. If the symptom persists, disable the SA-VAM2 by entering the **no crypto engine accelerator** command. Doing so causes the router to switch to software encryption.

Caveats Resolved Prior to Cisco IOS Release 12.3(11)YF2

The following caveats are resolved in Cisco IOS Release 12.3(11)YF1:

- CSCef57647—Incorrect PDSN CISCO-CDMA-PDSN-MIB Counter Values

On a Cisco router running R2.0 Packet Data Serving Node (PDSN) software, the CISCO-CDMA-PDSN-MIB counters “cCdmaActiveSessions”, “cCdmaDormantSessions”, and “cCdmaPcfSoRpUpdOtherReaReqs” show incorrect values.

Workaround: none.

- CSCef86875—PDSN Reloads While Disabling Conditional Debugging For Prepaid

On Cisco router running Release 2.1 PDSN software, the router reloads while disabling conditional debugging feature for Prepaid Accounting.

The symptom occurs when prepaid accounting is enabled with conditional debugging.

Workaround: none.

- CSCeg21567—**show cdma pdsn statistics ppp** - Wrong Release Counter Value

On a Cisco router configured for PDSN, the “release total” counter might increase by 2 instead of 1 in the output of **show cdma pdsn statistics ppp** command.

Workaround: none.

- CSCeg33664—PDSN Does Not Send AHDLC FF03 Fields for VPN Traffic

On Cisco Packet Data Service Node (PDSN), when VPDN calls are made from the Mobile Node (MN), the PDSN in the downstream path (packets destined to the mobile) does not include the Address and Control Field (ACF - FF03) in the packet.

Workaround: none.
- CSCin77352—[CRP]:Memory Leak While Opening and Closing CRP Sessions at 125 CPS

When closed RP sessions are opened and closed at a high rate on the PDSN, a memory leak occurs. This condition occurs only when closed RP sessions are opened and closed.

Workaround: none.
- CSCin86234—Add Message Authenticator Attribute for Prepaid Online Access Requests

The Cisco PDSN does not include a Message-Authenticator attribute in the online Access Requests that are being sent by prepaid sessions for quota retrieval.

Workaround: none.
- CSCin86235—Configuring **skip-aaa-reauth** Made the HA Fail MIP Registration

When the **ip mobile foreign-agent skip-aaa-reauthentication** command is configured, the **ip mobile foreign-agent nat traversal force** command also gets configured. This causes the initial RRQ from the PDSN to the HA to fail.

Workaround: unconfiguring the **ip mobile foreign-agent nat traversal force** command will help correct this.
- CSCsa44772—PDSN Should Not Send A11 Session Update if Current RNPDIIT <= Previous RNPDIIT

The Cisco PDSN sends session update message to PCF when the RN-PDIIT downloaded is less than RN-PDIIT stored.

This condition occurs when the second MIP flow is opened for a user and the same RN-PDIIT, Always-On values are downloaded from radius server.

Workaround: none.
- CSCsa45264—Last Character of Calling Station ID Stripped When PDSN Sends to LNS

On Cisco PDSN running 12.3(8)XW3, when VPDN flows are opened on the A11 session, the PDSN acting as LAC will send an ICRQ to the LNS. In the ICRQ message PDSN will include the Calling Station ID received in the A11 Registration Request. When the Calling Station ID is sent from PDSN, the last character of Calling Station ID is not encoded in the ICRQ to the LNS.

This condition occurs for all VPDN flows opened over the A11 session.

Workaround: none.
- CSCsa48683—MWAM Should Return cevC6xxxMWAMBlade When Queried for sysObjectID

The MWAM processor returns a sysObjectId of “ciscoWsSvcMWAM1” instead of “cevC6xxxMWAMBlade”. Because of this, the network management station running RME 4.0 may not be able to identify the device successfully.

This condition occurs when the MWAM processor is running a Cisco IOS image 123(11)YF, or later.

Workaround: none.

Caveats Resolved Prior to Cisco IOS Release 12.3(11)YF1

The following caveats are resolved in Cisco IOS Release 12.3(11)YF:

- CSCed65017—MWAM: Config CLI That Fail Batch Mode Copy Fail config-mode sup

Some configuration commands fail, do not operate properly, or cause dead memory when using batch mode config download or config-mode supervisor.

This problem occurs when the MWAM processor is configured for “supervisor” config-mode.

Workaround: use config-mode local on MWAM.
- CSCee45296—MWAM Does Not Retrieve its Configuration From the Supervisor

When using config on supervisor with the MWAM, the processors are not able to retrieve their configurations from the supervisor.

This problem was first seen when using supervisor release 122-18.2.2.SX. This defect would be present in all future supervisor releases when mated with an MWAM IOS image that did not contain this fix.

Workaround: configure an arbitrary tftp-server (for example, tftp-server nvram:startup-config) on the supervisor. It does not matter what file you serve up, even one of the MWAM configs. If you do serve up one of the MWAM configs, be sure to add the alias: “tftp-server bootflash:SLOTxPCy.cfg alias SLOTxPCy.cfg”.

Supervisor release 122-18.2.2.SX changed the mechanism used by the MWAM processors to retrieve their configurations. This DDTS changed the mechanism used by the MWAM processors to be compatible with the supervisor IOS change. This ddts is also backwards compatible with previous supervisor images.
- CSCef71485—MWAM Processor Reloads While Sending Certain Fragmented Packets

The MWAM reloads while sending fragmented downstream packets.

This problem occurs when you send downstream data with more fragmented packets.

Workaround: disable cef.
- CSCin79481—PDSN Reloads When Parsing a MSG_PENDING Selection Message From Peer

Cisco Packet Data Service Node (PDSN) Release 1.2 will reload when parsing a Messaging pending selection message from a peer participating in a peer-peer model of selection (under the condition explained below), if the PDSN address communicated in the message is not present in its load list.

This condition occurs when the Peer-Peer mode of selection with load balancing is enabled, and a PDSN receives a MSG_PENDING CVSE and the PDSN address communicated in the message is not present in its load list.

Workaround: disable load balancing in peer-peer mode of selection.

Resolved Caveats Prior to IOS Release 12.3(11)YF

The following caveats are resolved in Cisco IOS Release 12.3(8)XW3:

- CSCed86177—Tracebacks Found On PDSN With CEF and NAT Enabled for SIP flow

A Cisco router running 12.3T R2.0 Release PDSN software sometimes produces tracebacks while sending bidirectional traffic from mobile node to reflector in SIP flow with compress stack enabled and cef switched

This condition occurs while sending bidirectional traffic from mobile node to reflector in SIP flow with compress stack enabled and cef switched.

Workaround: none.
- CSCee13372—IPSec Tunnel Goes Down Before Receiving ACK for Revocation Request

When the last mobile tunnel binding is brought down on HA, a revocation message is sent from HA and CDMA IPSec tunnel is brought down without waiting for a revocation acknowledgement message from the PDSN.

This condition has been observed on a router that is running Cisco IOS release 12.3T software.

Workaround: none.
- CSCef50548—TOS Value Set to Non-Zero Value for PPP Control Packets

On Cisco router running Release 2.0 PDSN software, during Point to Point (PPP) negotiation, the IPCP control packets sent downstream to the Mobile Node from PDSN are encapsulated using GRE, and then sent to Mobile Node.

The DSCP marking on the Type of Service (TOS) filed in the outer header, was found to be a non-zero (Garbage) value.

This behavior is seen only when the PPP negotiations happens. If we send traffic over the established tunnel, those packets are marked with correct (TOS =0) value.

Workaround: none.
- CSCin77744—PDSN Drops Fragmented PCF Packets Intermittently

On the Packet Data Service Node (PDSN), when the Generic Routing Encapsulation (GRE) packets received from the Packet Control Function (PCF), they are dropped intermittently if the packets are fragmented.

Packets drops are seen on the PDSN when the PPP negotiation between the PDSN and Mobile Node Terminates the Compression Control Protocol (CCP), and then during the data transfer the Mobile Node sends another CCP ConfReq to the PDSN.

Workaround: By disabling compression on PDSN Virtual Template, packet drop was not observed
- CSCin81236—Conditional Debugging Skips Some RADIUS Msgs for MIP Flows

When conditional debugging is enabled on Cisco PDSN running 12.3(8)XW image, RADIUS related debugs are not shown sometimes for a Mobile IP flow that is opened on the box.

This condition occurs when conditional debugging is set for RADIUS related debugs.

Workaround: none.

- CSCin81520—Extra Mobile IP Debugs Are Printed for Conditional Debugging
Some extra mobile IP debugs are printed on Cisco PDSN running 12.3(08)XW software when mobile IP conditional debugging is enabled on it. Debugs that get printed are not corresponding to the user.
This condition occurs when conditional debugging for Mobile IP is turned on.
Workaround: none.

Resolved Caveats Prior to IOS Release 12.3(8)XW3

The following caveats are resolved in Cisco IOS Release 12.3(8)XW2:

- CSCed86144—Tracebacks Found in Clustering
Cisco router running Packet Data Serving Node (PDSN) Software in redundant cluster controller member environment may show tracebacks on active controller and may lead to a reload.
This condition occurs under a rare condition when controllers are present in redundancy environment with active and standby controller and simple IP sessions are opened. On the active controller preemption is enabled and this has the higher priority. If active is brought down and recovers, when it tries to take control back from the standby, tracebacks may appear on active controller and may lead to a reload.
Workaround: Disable preemption on the active controller.
- CSCee18749—PDSN deletes only a single flow when POD received
When the Cisco Packet Data Service Node (PDSN) has multiple MIP flows for the same user and receives a Packet of Disconnect (POD) request with IMSI for the user, it deletes only a single flow for the IMSI. One flow for the IMSI is deleted each time the POD request is resent.
This problem is only seen when multiple flows with the same username exists for the session.
Workaround: none.
- CSCee31554—ODAP Lease Renewal Out of Sync on Active and Standby
On Cisco 7600 running HA Release 2.0 image, lease time is not sync on Active and Standby HA's. This will result into out of sync between Active and Standby HA.
Open 25 k bindings on active and standby HA reload active mwam standby HA become active, and try to renew lease, some subnets are out of sync with server. Unable to renew lease. Server is deleting subnets after lease expiry. Due to this both active and standby bindings are deleted
Workaround: none.
- CSCee81662—PPP May Get Stuck in TERMSSENT in High CPU Situation
PPP sessions may get stuck in the TERMSSENT state. This symptom is observed on a Cisco platform that has a high CPU utilization.
Workaround: Clear the underlying layer (VPDN, PPPoA, or PPPoE).
- CSCef09658—Tracebacks [Spurious Memory] Seen in the Standby Controller.
Tracebacks were seen when a standby controller was added to the cluster.
Workaround: none.

- CSCef18987—POD Debugs Display NACK Error Message For a Valid POD Request
A Cisco PDSN running R2.0 S/W incorrectly displays a NACK message being sent even though it correctly sends an ACK message to RADIUS server in response to a POD request.

This condition occurs when the POD feature is enabled, and the PDSN receives a POD request from RADIUS server with only NAI and NAS-ID and no session identification attributes in it.

Workaround: none

- CSCef19117—**ip tcp adjust-mss** Command Fails to Set Value for Outbound Packets
Cisco router configured with the **ip tcp adjust-mss** command may fail to set the value for outbound packets.

The command works on 12.3(7)T2 code, but fails on 12.3(8)T code. This issue is currently seen on a 3700 router.

Workaround: disable cef.



Note This can affect the router performance. This issue is not seen with cef disabled on the router.

- CSCef25623—PDSN Reloads While Unconfiguring Cluster Member Interface
A Cisco router running 12.3(7)T3 R1.2 Release of the PDSN software reloads when you unconfigure the **cdma pdsn cluster member interface** command.

Workaround: none.

- CSCee31554—ODAP Lease Renewal Out Of Sync on Active and Standby

On a Cisco 7600 running the HA R2.0 Image, the lease time is not synchronized on active and standby HAs. This causes the active and standby HAs to be out of sync.

The following conditions must exist for this problem to occur:

- Open 25k bindings on active and standby HA.
- Reload active MWAM.
- Standby HA become Active, and try to renew lease.
- Some subnets are out of sync with server. Unable to renew lease. Server is deleting subnets after lease expiry. Due to this, both active and standby bindings are deleted

Workaround: none.

- CSCef39286—Incorrect Tunnel Endpoint for PMIP Flows While Using HA-SLB.

On Cisco router running Release 2.0 PDSN software, when Proxy MIP flow is opened in a setup with HA-SLB, the MIP tunnel endpoint for the session on the PDSN is incorrect. This causes re-registrations and data transfer through this session to fail.

This symptom occurs when Proxy MIP flow is opened with HA-SLB. This issue is not seen when HA SLB is not used.

Workaround: none.

- CSCef59046—Crashed By Bus Error When Issuing IP Mobile

The router reloaded by bus error when the customer issued command **no ip mobile host nai @xxx.xxx.xxx.xxx address pool local ha-pool interface FastEthernet x/x aaa** after configuring **ip mobile host nai @xxx.xxx.xxx.xxx address pool local ha-pool interface FastEthernet x/x aaa**.

Workaround: none.

- **CSCin78876—MIP CPS Low With MobileIP Global Configuration**
On a Cisco Packet Data Service Node (PDSN), when Mobile IP flows are opened at the rate of 1000 cps, some of Mobile IP flows are closed.
This occurs when the Mobile IP registration lifetime in the Registration Request is not INFINITE (65535).
Workaround: none.
- **CSCin79040—CPS Degradation on Configuring Accounting Start-Stop**
On Cisco Packet Data Serving Node (PDSN), calls per second on a cluster of 8 Members and 2 Controllers is lower than the PRD requirement.
Workaround: none.
- **CSCin80761—PDSN Does Not Set Proper PPP Call Fail Reason For Authentication Fail**
Cisco Packet Data Service Node (PDSN) Rel 1.2 sends an invalid PPP call fail reason for authentication fail scenario.
This condition occurs when sending of PPP call fail reason to a Proprietary PCF is enabled and MN fails authentication in PPP authentication phase.
Workaround: none.

Related Documentation

Except for feature modules, documentation is available as printed manuals or electronic documents. Feature modules are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- [Release-Specific Documents, page 61](#)
- [Platform-Specific Documents, page 62](#)
- [Feature Modules, page 62](#)
- [Cisco IOS Software Documentation Set, page 62](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3T:

- *Packet Data Serving Node (PDSN) Release 2.1* at the following url:
http://www.cisco.com/en/US/products/sw/wirelssw/ps4341/tsd_products_support_series_home.html

The following documents are specific to Release 12.3 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.3*

On CCO at:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes

- *Caveats for Cisco IOS Release 12.3 T*

See *Caveats for Cisco IOS Release 12.3T*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.3.

On CCO at:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Caveats



Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco Bug Toolkit: Cisco Bugtool Navigator II**, or at <http://www.cisco.com/support/bugtools>.

- Product bulletins, field notices, and other release-specific documents on CCO at:

Technical Documents

Platform-Specific Documents

Documentation specific to the Cisco 7206 Router is located at the following locations:

- On Cisco.com at:
http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_series_home.html

Documentation specific to the Cisco 7600 Router is located at the following location:

- On Cisco.com at:
http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

Documentation specific to the Cisco Catalyst 6500 Switch is located at the following location:

- On Cisco.com at:
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Feature Modules

Feature modules describe new features supported by Release 12.3 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On CCO at:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.3: New Feature Documentation

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM, unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On CCO at:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

Release 12.3 Documentation Set

[Table 3](#) describes the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form when ordered.



Note

You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.3

Table 3 *Cisco IOS Software Release 12.3 Documentation Set*

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	<ul style="list-style-type: none"> Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management
<ul style="list-style-type: none"> • <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i> 	<ul style="list-style-type: none"> Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking

Table 3 Cisco IOS Software Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i> • <i>Cisco IOS Dial Services Configuration Guide: Network Services</i> • <i>Cisco IOS Dial Services Command Reference</i> 	<ul style="list-style-type: none"> Preparing for Dial Access Modem Configuration and Management ISDN and Signalling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Interworking Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	<ul style="list-style-type: none"> Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP and IP Routing Configuration Guide</i> • <i>Cisco IOS IP and IP Routing Command Reference</i> 	<ul style="list-style-type: none"> IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	<ul style="list-style-type: none"> AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	<ul style="list-style-type: none"> Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Multiservice Applications Configuration Guide</i> • <i>Cisco IOS Multiservice Applications Command Reference</i> 	<ul style="list-style-type: none"> Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	<ul style="list-style-type: none"> Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signalling Link Efficiency Mechanisms Quality of Service Solutions

Table 3 Cisco IOS Software Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching MPLS Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
<ul style="list-style-type: none"> • <i>New Features in 12.3-Based Limited Lifetime Releases</i> • <i>New Features in Release 12.3 T</i> • Release Notes (Release note and caveat documentation for 12.3-based releases and various platforms) • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Dial Services Quick Configuration Guide</i> 	

**Note**

Cisco Management Information Base (MIB) User Quick Reference is no longer published. If you have an account with CCO, you can find the current list of MIBs supported by Cisco. To reach the *Cisco Network Management Toolkit*, go to CCO, press **Login: Technical Support: Software Center: Network Mgmt Software: Cisco Network Management Toolkit: Cisco MIBs**.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

Copyright © 2008, Cisco Systems, Inc.
All rights reserved.