



Release Notes for the Cisco PDSN 2.1 Feature in Cisco IOS Release 12.3(11)YF2

May 2005

Cisco IOS Release 12.3(11)YF2 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. Cisco IOS Release 12.3(11)YF2 is optimized for the Cisco PDSN Release 2.1 feature on the Cisco 7206VXR router, the Cisco 7206VXR Router with Cisco NPE-G1 Network Processing Engine, the Cisco 7609 Internet Router, and the MWAM card on the Cisco 6500 Catalyst Switch platform and 7600 Internet router platform.

Contents

These release notes include important information and caveats for the Cisco PDSN software feature provided in Cisco IOS 12.3(11)YF2 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/univercd/cc/td/doc/product/software/ios123/index.htm>

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

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/7000/index.htm>

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

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123reInt/cat6000/index.htm>

This release note includes the following topics:

- [System Requirements, page 2](#)
- [Packet Data Serving Node Software Features in Release 12.3\(11\)YF2, page 5](#)
- [Caveats, page 6](#)
- [Related Documentation, page 28](#)
- [Obtaining Documentation, page 33](#)
- [Obtaining Technical Assistance, page 33](#)



Corporate Headquarters:

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

Copyright © 2003. Cisco Systems, Inc. All rights reserved.

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, 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(11)YF2:

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

Memory Requirements

[Table 1](#) shows the memory requirements for the PDSN Software Feature Set that supports the Cisco 7206VXR router, the Cisco 7206VXR Router with Cisco NPE-G1 Network Processing Engine, the Cisco 7609 Internet Router, and the MWAM card on the Cisco 6500 Catalyst Switch platform and 7600 Internet router platform. 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.123-11.YF2 c7200-h1is-mz.123-11.YF2 c7200-c6ik9s-mz.123-11.YF2 c7200-h1ik9s-mz.123-11.YF2	20 MB	512 MB	RAM
Cisco 6500 Catalyst Switch	PDSN Software Feature Set	c6svcmwam-2.1.2.0-c6is-123-11.YF2-5cpu.bin (This is a bundled image) svcmwam-c6is-mz.123-123-11.YF2	40MB	512MB	RAM
Cisco 7600 Internet Router	PDSN Software Feature Set	c6svcmwam-2.1.2.0-c6is-123-11.YF2-5cpu.bin (This is a bundled image) svcmwam-c6is-mz.123-123-11.YF2	40MB	512MB	RAM
Cisco 7206VXR Router with NPE-G1	PDSN Software Feature Set	c7200-c6is-mz.123-11.YF2 c7200-h1is-mz.123-11.YF2 c7200-c6ik9s-mz.123-11.YF2 c7200-h1ik9s-mz.123-11.YF2	40MB	512MB	RAM

Hardware Supported

Cisco IOS Release 12.3(11)YF2 is optimized for PDSN Release 2.1 on the Cisco 7206VXR router, the Cisco 7206VXR Router with Cisco NPE-G1 Network Processing Engine, the Cisco 7609 Internet Router, and the MWAM card on the Cisco 6500 Catalyst Switch platform and 7600 Internet router platform.

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(11)YF2 is a special release that is developed on Cisco IOS Release 12.3.

Cisco IOS Release 12.3(11)YF2 supports the same features that are in Cisco IOS Release 12.3, with the addition of the PDSN Release 2.1 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
Cisco Internetwork Operating System Software
IOS (tm) MWAM Software (MWAM-C6IS-M), Version 12.3(11)YF, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)Synched to technology version 12.3(8)T
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by cisco Systems, Inc.
```

Upgrading to a New Software Release

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(11)YF2 supports the same feature sets as Cisco Release 12.3, with the exception that Cisco Release 12.3(11)YF2 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(11)YF2

The Cisco IOS Release 12.3(11)YF2 supports the same feature sets as Cisco Release 12.3, with the exception that Cisco Release 12.3(11)YF2 includes the PDSN feature. The PDSN 2.1 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:

- 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
- On-Demand Address Pools (ODAP)
- 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
- PDSN Clustering Peer-to-Peer and Controller / Member Architecture

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/univercd/cc/td/doc/product/software/ios123/index.htm>

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/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123t/123tcavs.htm>

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(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 Nosetup

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 nosetup 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 Torndown 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(11)YF2:

- CSCef67682— IPv6 msg cause trackback

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

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

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

This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognises as its own. This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

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

- CSCef68324

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

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

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

- 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
Tunnell 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.

- CSCsa54608

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

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

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

Only devices running certain versions of Cisco IOS are affected.

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

This advisory will be posted at

http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml

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 ddt changed the mechanism used by the MWAM processors to be compatible with the supervisor IOS change. This ddt 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 behaviour is seen only when the PPP negotiations happens. If we send traffic over the established tunne, 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 28](#)
- [Platform-Specific Documents, page 29](#)
- [Feature Modules, page 29](#)
- [Cisco IOS Software Documentation Set, page 29](#)

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/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123yf/123yf11/pdsn21/index.htm>

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 CCO at: <http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/index.htm>

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

- On CCO at: <http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/index.htm>

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

- <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm>

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> 	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> 	Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking
<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> 	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> 	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces

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

Books	Major Topics
<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
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	<ul style="list-style-type: none"> 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> 	<ul style="list-style-type: none"> 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

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

Books	Major Topics
<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

World Wide Web

You can access the most current Cisco documentation on the World Wide Web (WWW) at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides CCO as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center (TAC). All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many Cisco printed documents, or by sending mail to Cisco.

Cisco Connection Online

CCO is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
 - From North America, call 408 526-8070
 - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco TAC is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use <http://www.cisco.com/public/support/tac>.

To contact by e-mail, use one of the following addresses:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/technotes/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Technical Assistance Center: Technical Tips**.

The following sections are provided from the Technical Tips page:

- **Access Dial Cookbook**—Contains common configurations or recipes for configuring various access routes and dial technologies.
- **Field Notices**—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- **Frequently Asked Questions**—Describes the most frequently asked technical questions about Cisco hardware and software.
- **Hardware**—Provides technical tips related to specific hardware platforms.
- **Hot Tips**—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- **Internetworking Features**—Lists tips on using Cisco IOS software features and services.
- **Sample Configurations**—Provides actual configuration examples that are complete with topology and annotations.

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

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