Release Notes for the Cisco PDSN 4.1 Feature in Cisco IOS Release 12.4(15)XR10

Published: May 2011, OL-23064-02

Cisco IOS Release 12.4(15)XR10 is based on Cisco IOS Release 12.4, with enhancements to the Cisco Packet Data Serving Node (Cisco PDSN) feature. This Cisco PDSN Release 4.1 update based on IOS Release 12.4(15)XR10 is optimized for the Cisco PDSN feature on the Cisco Service and Application Module for IP (SAMI) card on the Cisco 7609 Series Router.

Contents

These release notes include important information and caveats for the Cisco PDSN software feature provided by Cisco IOS 12.4(15)XR10 for the Cisco 7609 Series Router platform.

This release note describes:

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

Introduction

Cisco PDSN is an IOS software feature that enables a Cisco SAMI card on a Cisco 7600 Series 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 intranet, or Wireless Application Protocol (WAP) services. Cisco PDSN supports both simple IP and mobile IP operations.

System Requirements

This section describes the system requirements for running Cisco IOS Release 12.4(15)XR10 to support Cisco PDSN 4.1:

Memory Requirements

To install Cisco PDSN 4.1 that supports the SAMI card on the Cisco 7600 Series Router, ensure that you meet the following memory requirements:

- Platform: Cisco 7600 Series Router
- Bundled Image Filename: *12.4(15)XR- c7svcsami-c6ik9s-mz.124-15.XR10*
- Required Memory:
  - Flash: 256 MB
  - DRAM: 2048 MB

Hardware Supported

Cisco IOS Release 12.4(15)XR10 is optimized for the SAMI card on the Cisco 7600 Series Router. You can use the Hardware-Software Compatibility Matrix tool to search for hardware components that are supported on a Cisco platform and an IOS release.

Note You must have a valid Cisco.com account to log in to this tool: http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Software Compatibility

Cisco IOS Release 12.4(15)XR10 is developed on Cisco IOS Release 12.4 and supports the features included in Cisco IOS Release 12.4(15)T, with the addition of the Cisco PDSN feature.

For information on the new and existing features, see Cisco PDSN Software Features in Release 12.4(15)XR10.

MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs have been converted to more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update deprecated MIBs to the replacement MIBs, as shown in Table 1.

Table 1 Deprecated and Replacement MIBs

Deprecated MIB	Replacement MIB
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-CISCO-* 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

Migration to Cisco PDSN

This section describes the migration paths and scenarios for Cisco PDSN 4.1:

Migration Path for Cisco PDSN

Table 2 lists currently available Cisco PDSN releases and the migration path to the SAMI card.

:

Table 2 Migration Path for Cisco PDSN

	PDSN 3.0 or earlier	PDSN 3.5	PDSN 4.0
Platform	• 7200 NPE400/NPE-G1 • MWAM platform (5 processors only)	MWAM (5 processors only)	SAMI
Chassis/Power Supply, Fan Trays	7200VXR	• 6500 chassis • 7600 chassis	7600 chassis
Supervisor Engine	—	• SUP2 • SUP720	• SUP720 • RSP720 • SUP 32
Supervisor Engine	—	• SUP32 • SUP IOS SX-based	SUP IOS SRC-based image (for example: *c7600s72033-advipservicesk9-mz.122-33.SRC.bin*)
—	—	SUP redundancy	SUP redundancy

Migration Scenarios for Cisco PDSN 4.1

Based on Table 2, there are many possible migration scenarios. This section focuses on those scenarios that are closest to existing customer deployments. You must determine the migration path based on your end-to-end deployment.

Note We recommend that you perform the migration during a maintenance window in your deployment. You can also use this window for the following network redesign activities:

- Redesigning IP address scheme.
- Configuring the routing protocols.
- Configuring network connectivity between Cisco PDSN and the Home Agent (HA).
- Configuring application connectivity between Cisco PDSN and AAA servers.
- Configuring routing on the new SAMI Cisco PDSN or the HA.

Note For all the migration plans, both hardware and software configurations have significant changes. This requires prudent operation planning and network redesign. The Migration Steps section describes possible migration steps to minimize both network reconfiguration and service disruption.

Table 3 lists the most common migration scenarios.

Table 3 Migration Scenarios for Cisco PDSN 4.1

Scenario	Migration From	To	Remarks	Downtime
1	• Non-SR • Non- clustering • Single 7200VXR/NPE-G1 running Cisco PDSN	• Non-SR • Non-clustering • 7600 chassis • One SUP720/SAMI (Fewer than six PPC) running Cisco PDSN	Significant network provisioning changes in terms of: • Platform change • Configuration related to platform • Configuration related to Cisco PDSN provisioning (for example, creation of subinterfaces, VLAN, PCF secure configurations, and so on). • Configuration migration from 7200 to SAMI processor **Note** The majority of the basic configuration tasks related to the CDMA component remains the same, unless you plan to introduce features that were disabled before migration.	Yes
2	• Non-SR • Non-clustering • Multiple 7200VXR/NPE-G1s running Cisco PDSN	• Non-SR • Non-clustering • 7600 chassis • One SUP720/SAMI (all six PPC) running Cisco PDSN	Significant network provisioning change in terms of: • Platform change • New configuration related to platform (SUP/SAMI) • Configuration related to Cisco PDSN provisioning (for example, creation of subinterfaces, VLAN, PCF secure configurations, and so on). • Configuration migration from 7200 to SAMI processor **Note** The majority of the basic configuration tasks related to the CDMA component remains the same, unless you plan to introduce features that were disabled before migration.	Yes

Table 3 Migration Scenarios for Cisco PDSN 4.1 (continued)

Scenario	Migration From	To	Remarks	Downtime
3	• Non-SR • Non-clustering • IPsec enabled between 7200-based Cisco PDSN and HA • Two 7200VXR/NPE-G1 running Cisco PDSN	• SR enabled • Non-clustering • 7600 chassis • SUP720 blade with redundancy • IOS-based IPsec feature enabled • Two SAMI blades (single chassis)	Significant network provisioning change in terms of: • Platform change • New configuration related to platform (SUP/SAMI) • Crypto settings to be configured at Supervisor, instead of Cisco PDSN processors. IPsec tunnel to be established between 7600 chassis running Cisco PDSN and HA application, instead of terminating the IPsec tunnels in Cisco PDSN/HA application (similar to that of the 7200 platform). • Configuration related to Cisco PDSN provisioning (for example, creation of subinterfaces, VLAN, PCF secure configurations, and so on). • Configuration migration from 7200 to SAMI processor. **Note** The majority of the basic configuration tasks related to the CDMA component remains the same, unless you plan to introduce features that were disabled before migration.	Yes

Table 3 Migration Scenarios for Cisco PDSN 4.1 (continued)

Scenario	Migration From	To	Remarks	Downtime
4	• SR enabled • Non-clustering • 7600/Redundant SUP2 • Redundant MWAM blades (single chassis)	• SR enabled • Non-clustering • 7600/Redundant SUP720 • Redundant SAMI blades (single chassis)	Minimal changes in terms of hardware: • Platform upgrade (SUP2 to SUP720) requiring chassis reset. • New configuration related to SAMI platform to be enabled in SUP. • Configuration migration from MWAM processor to SAMI processor. **Note** The majority of the basic configuration tasks related to the CDMA component remains the same, unless you plan to introduce features that were disabled before migration.	Yes
5	• SR enabled • Non-clustering • 7600/Redundant SUP720 • Redundant MWAM blades (single chassis) • SUP IOS SXF	• SR enabled • Non-clustering • 7600/Redundant SUP 720 • Redundant SAMI blades (single chassis) • SUP IOS SRC	Minimal changes in terms of hardware: • SUP image upgrade (SXF to SRC) requiring chassis reset. • New configuration related to SAMI platform to be enabled in SUP. • Configuration migration from MWAM processor to SAMI processor. **Note** The majority of the basic configuration tasks related to the CDMA component remains the same, unless you plan to introduce features that were disabled before migration.	Yes

Table 3 Migration Scenarios for Cisco PDSN 4.1 (continued)

Scenario	Migration From	To	Remarks	Downtime
6	• SR enabled • Non-clustering • 7600/Redundant SUP720 • Redundant MWAM blades (single chassis) • SUP IOS SXF	• SR enabled • Clustering enabled • 7600/Redundant SUP720 • Redundant SAMI blades (single chassis) • SUP IOS SRC	Minimal changes in terms of hardware: • SUP image upgrade (SXF to SRC) requiring chassis reset. • New configuration related to SAMI platform to be enabled in SUP. • Configuration migration from MWAM processor to SAMI processor. • Provisioning of clustering setup requires introducing clustering-related configurations in Cisco PDSN processor, controller configuration, and PCF configuration changes. **Note** We recommend that you allow the controller and member to operate in different subnets. **Note** The majority of the basic configuration tasks related to the CDMA component remains the same, unless you plan to introduce features that were disabled before migration.	Yes

Table 3 Migration Scenarios for Cisco PDSN 4.1 (continued)

Scenario	Migration From	To	Remarks	Downtime
7	• SR enabled • Clustering enabled • 7600/Redundant SUP720 • Redundant MWAM blades (single chassis) • SUP IOS SXF	• SR enabled • Clustering enabled • 7600/Redundant SUP720 • Redundant SAMI blades (dual chassis) • SUP IOS SRC	Significant changes in terms of hardware: • SUP image upgrade (SXF to SRC) requiring chassis reset. • Introduction of redundant chassis. • Provisioning of the SUP configuration to operate in an inter-chassis redundant environment. • New configuration related to SAMI platform to be enabled in SUP. • Configuration migration from MWAM processor to SAMI processor. • Provisioning of clustering setup requires introducing clustering-related configurations in the Cisco PDSN processor, controller configuration, and PCF configuration changes. **Note** The majority of the basic configuration tasks related to the CDMA component remains the same, unless you plan to introduce features that were disabled before migration.	Yes

Migration Steps

Migration to the Cisco PDSN Release 4.1 image is more than replacing Multi-processor WAN Application Module (MWAM) cards with SAMI modules. Ensure that you plan your migration such that migration activities have a minimal impact on an existing mobile subscriber's service connections.

Table 4 lists the migration tasks that are based on the scenarios established in the previous section.

Table 4 Migration Steps from Cisco PDSN 3.x to 4.1

Scenario	Migration Steps
1, 2	• Install and configure Cisco PDSN on 7600/SUP720 (SRC based) with the SAMI. • Provision Mobile Station (MS) and Packet Control Functions (PCF) to use the newly added SAMI-based Cisco PDSN (this provisioning may take an extended period of time to complete). • Provision newly added Cisco PDSN with that of HA to service mobile IP calls. Also, modify the security association between Cisco PDSN and PCFs, and Cisco PDSN and the HA, accordingly. • To minimize provisioning tasks (assuming that the migration is done in a maintenance window and that service will be disrupted) , the SAMI Cisco PDSN instances can reuse the 7200 NPE-G1-based Cisco PDSN IP addresses and routing schemes.
3	• Install and configure the Cisco PDSN on 7600/SUP720 (SRC based) with the SAMI, and locate them in the same HSRP redundancy group as configured on the Cisco 7200-based Cisco PDSN (Release 3.0). At this stage, the Cisco 7200-based Cisco PDSN will act as the active Cisco PDSN and the SAMI-based Cisco PDSN will assume the role of standby. • Ensure in the newly introduced SAMI-based Cisco PDSN, that Release 3.5 or Release 4.0 features are not enabled. Also, ensure that the features enabled on the SAMI Cisco PDSN match the features already enabled on the 7200-based Cisco PDSN. However, the IPsec feature enabled on the 7200 Cisco PDSN must be disabled on a SAMI-based Cisco PDSN. Instead, the IPsec configuration will be moved to the 7600 Supervisor configuration, and the IPsec tunnel will be established between the chassis. After the packet is taken out of the IPsec tunnel in the Supervisor, the packet is sent to Cisco PDSN instances through the backplane. • Configure higher priority and Hot Standby Router Protocol (HSRP) preemption (with delay) on the SAMI-based Cisco PDSN. • The SAMI Cisco PDSN takes over the active role. • Bring down Cisco 7200s and introduce another SAMI card (SAMI card 2) in the same chassis to configure redundancy. Enable the SAMI card 2 to take over the role of standby Cisco PDSN. **Note** Customers usually prefer to reconfigure their network in a maintenance window, so we continue to recommend the same for this configuration change as well. However, it is not required that you perform this step in a maintenance window. Introducing new features (such as those in Release 4.1), however, must be done only during a maintenance window.

Table 4 Migration Steps from Cisco PDSN 3.x to 4.1

Scenario	Migration Steps
4	• Install and configure Cisco PDSN on 7600/SUP720 (SRC based) with the SAMI and locate them in the same HSRP redundancy group as configured on the MWAM-based Cisco PDSN (Release 3.0). At this stage, the MWAM Cisco PDSN instances act as the active Cisco PDSN and the SAMI-based Cisco PDSN assumes the role of standby. **Note** The SAMI card can be configured for six instances of Cisco PDSN, whereas the MWAM has only five instances. Customers can efficiently provision the network and distribute the load across six Cisco PDSN instances (instead of five) during the upgrade process. • Configure SUP720 to support SAMI. – Ensure MWAM configurations are saved on the SUP720 bootflash. – Configure the VLAN for SAMI VLAN groups on SUP720 as MWAM. – Build the SAMI PPC configuration from MWAM processors configurations according to the SAMI configuration filename convention in the SUP720 bootflash. – Power down the standby MWAM and remove it from the chassis. – Insert the SAMI in the same slot and boot it with the Cisco PDSN Release 4.1 image. – Verify that the SAMI PPC receives the proper Cisco PDSN configurations. • Ensure that the newly introduced SAMI-based Cisco PDSN does not enable any of the Release 3.5 or Release 4.0 features. Also, ensure that the features enabled on the SAMI Cisco PDSN match the features already enabled on the MWAM-based Cisco PDSN. • Configure higher priority and HSRP preemption (with delay) on the SAMI-based Cisco PDSN. • The SAMI Cisco PDSN takes over the active role. • Bring down the standby MWAM and introduce another SAMI card (SAMI card 2) in the same chassis and configure redundancy. Enable the SAMI card 2 to take over the role of standby Cisco PDSN. **Note** Customers usually prefer to reconfigure their network in a maintenance window, so we continue to recommend the same for this configuration change. However, it is not required that you perform this step in a maintenance window. Introducing new features (such as those in Release 4.1), however, must be done only during a maintenance window.
5	• For a single chassis, changing from SUP720 SXF to SUP720 SRB resets the entire chassis. The whole chassis is reset, so all service modules such as MWAM and SAMI are reset too. This behavior is identical for SUP2 to SUP720, or SUP32 to RSP720 migration. ⚠ **Caution** Ensure that you perform this step during a maintenance window because user service will be disrupted. • For MWAM to SAMI Cisco PDSN migration, follow the steps given in Scenario 4.

Table 4 Migration Steps from Cisco PDSN 3.x to 4.1

Scenario	Migration Steps
6	• Because the SAMI blade does not support inter-PPC communication on the same VLAN, the existing cluster-member architecture model of the Cisco PDSN on a single MWAM blade requires configuration changes during provisioning using the SAMI platform. (Of five processors in the MWAM, one is used as controller and the others are used as a Cisco PDSN member.) You must use the IP address from a different subnet on the controller and member interface, and explicitly enable routing through the supervisor for communication with each other. **Note** This step requires additional configuration on the PCF side as well: change in cluster controller IP address in PCF, routing, and so on. • Additionally, ensure that the cluster-related configuration is newly introduced in the Cisco PDSN member for the member to participate in a cluster environment. • Complete the migration procedure using the steps described in scenario 4 or 5. **Note** You must perform this step in a maintenance window.
7	• The migration steps are similar to scenario 5. **Note** We do not recommend having MWAM (Release 3.0 image) and SAMI Cisco PDSN (Release 4.0 image) members participating in the same cluster controller based on Release 3.0 image for the following reasons: – Handling of Rev. A calls: Enabling the CLI to support multiple flows cannot be done in a Release 3.0-based controller. Additionally, having a SAMI and an MWAM Cisco PDSN participating in a single controller may end up redirecting or suggesting the IP address of a MWAM Release 3.0 Cisco PDSN for a Rev. A call.

Upgrading to New Software Release

The following sections describe how to determine the existing software version and how to upgrade your Cisco PDSN:

For information on upgrading to a new software release, see the product bulletin 957 *Cisco IOS Software Upgrade Ordering Instructions*, located at:

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

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** command in the EXEC mode:

```
Router# show version
Cisco IOS Software, SAMI Software (SAMI-C6IK9S-M), Experimental Version
12.4(20090828:113927) [sgontla-dtho_xr7 102]
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Fri 28-Aug-09 17:09 by sgontla

ROM: System Bootstrap, Version 12.4(15r)XQ1, RELEASE SOFTWARE (fc1)

mwtcp_ftb9-pdsn-93 uptime is 9 minutes
System returned to ROM by SUP request at 17:40:14 UTC Tue Aug 18 2009
System restarted at 14:04:25 UTC Mon Aug 31 2009
System image file is "c7svcsami-c6ik9s-mz.xr7-dtho"

This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html.

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco Systems, Inc. SAMI (MPC8500) processor (revision 2.2) with 786432K/262144K bytes of
memory.
Processor board ID SAD114203KX
FS8548H CPU at 1250MHz, Rev 2.0, 512KB L2 Cache
1 Gigabit Ethernet interface
65536K bytes of processor board system flash (AMD S29GL256N)

Configuration register is 0x2102

Router#
```

Upgrading the Supervisor Image

To upgrade the Supervisor image:

Step 1 Copy the SUP image to the disks (for example, disk0: / slavedisk0:).

Step 2 Add the following command to the running-configuration boot system disk0: *SUP-image-name*. For example:

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

Note To enable the image to reload, remove previously configured instances of this command.

Step 3 Run the **write memory** command to save the running-configuration on the active and standby SUP.

Step 4 Run the **reload** command on the active SUP.

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

Running the **reload** command on the active SUP causes both the active and standby Supervisors to reload simultaneously, causing some downtime during the upgrade process.

Upgrading the SAMI Software

To upgrade an Cisco PDSN image on the SAMI card, follow the directions at:

http://www.cisco.com/en/US/docs/wireless/service_application_module/sami/user/guide/maintain.html#wp1047551

Changing Configuration on Cisco PDSN in a Live Network

To change the working configuration on a Cisco PDSN in a live environment:

Step 1 Bring the standby Cisco PDSN out of service.

For example, to isolate the standby Cisco PDSN from the session redundancy setup, you must run the **no cdma pdsn redundancy** command.

```
7600a-Stdy(config)# no cdma pdsn redundancy
```

Step 2 Run the **write memory** command to save the configuration.

Step 3 Make the necessary configuration changes on the standby Cisco PDSN, and save the configuration.

Step 4 Run the **cdma pdsn redundancy** command again and save the configuration.

Step 5 Issue the **reload** command to bring the standby Cisco PDSN back into the session redundancy setup with the changed configuration. Verify if the processor comes back in the session redundancy 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 Configure the standby Cisco PDSN to take over as active by reloading the current active Cisco PDSN.

Caution Before proceeding with the configuration changes, we recommend that you disable the HSRP preemption configuration on the active and standby PDSN.
Because of a change of configuration following this step, an outage may occur on existing calls on the active PDSN (which is now being taken out of service) when synchronized with new active units.

Step 7 Configure the current standby PDSN using the procedure described from Step 1 to Step 5.

Note For Cisco PDSN session redundancy to work properly, ensure that configurations on the active and standby Cisco PDSNs are identical.

Cisco PDSN Software Features in Release 12.4(15)XR10

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.

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 or 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.

Cisco IOS Release 12.4(15)XR10 supports the same feature sets as Cisco Release 12.4; additionally, it supports the Cisco PDSN feature. Cisco PDSN 12.4(15)XR10 is optimized for the SAMI card on the Cisco 7600 Router, and includes the following new and existing features:

- Attribute support
  - Served MDN
  - Framed pool
  - 3GPP2 DNS server IP
- Virtual Route Forwarding (VRF) with subinterfaces support
- Conditional debugging enhancements for Cisco PDSN Release 4.1
- IOS 5.0 call flow for HRPD
- QoS features based on IS-835-D
- Per-flow accounting
- MIB enhancements
- Call Admission Control (CAC)
- Home area, maximum authorized aggregate bandwidth, and inter-user priority attributes downloaded from AAA
- Mobile Equipment Identifier (MEID) support
- Simple IPv6 access
- Session redundancy infrastructure
- RADIUS server load balancing
- Closed-RP or open-RP integration
- Domain-based subscriber authorization
- PPP counters
- RP counters
- 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
- Cisco PDSN cluster controller or member architecture

- Cisco PDSN MIB enhancement
- Cisco proprietary prepaid billing
- 3DES 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

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 12.4 are available on Cisco.com 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; they might also apply to previous releases.

The "Resolved Caveats" section lists caveats resolved in a particular release that may have been open in previous releases.

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

Open Caveats

Unresolved Caveats in Cisco IOS Release 12.4(15)XR10

There are no unresolved caveats in 12.4(15)XR10.

Unresolved Caveats in Cisco IOS Release 12.4(15)XR9

- CSCte14603

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtf17624

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtf91428

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

There are no unresolved caveats in the following releases:

- Cisco IOS Release 12.4(15)XR7
- Cisco IOS Release 12.4(15)XR6
- Cisco IOS Release 12.4(15)XR5
- Cisco IOS Release 12.4(15)XR4
- Cisco IOS Release 12.4(15)XR3

Unresolved Caveats in Cisco IOS Release 12.4(15)XR2

The following caveats are unresolved in Cisco IOS Release 12.4(15)XR2:

- CSCsv51151—For mobile IP Calls G15 and G16 for IP Flows in Not Sent Correctly

  For mobile IP calls, G15 and G16 for IP flows are incorrectly sent. When a session is closed for IP flows, G15 and G16 send the same values as the session.

  This issue occurs after the following steps:

  - A mobile IP session is opened with forward and reverse IP flows.
  - TFT is installed with forward and reverse packet filters (for opened IP flows).
  - The session is closed.

  Workaround: None.

- CSCsv23569—Domant-Dormant Handoff f1-f2, f6-f10, f14 are incorrectly sent to new PCF

  After performing a dormant-dormant handoff, f1-f2, f6-f10, and f14 are sent as non-zero values in accounting records for the new PCF.

  This issue occurs after the following steps:

  - A session is opened.
  - The session is made dormant by sending an active stop from the PCF.
  - A dormant-dormant handoff is performed.

  Workaround: None.

Unresolved Caveats in Cisco IOS Release 12.4(15)XR1

The following caveat is unresolved in Cisco IOS Release 12.4(15)XR1:

- CSCsu89978—Packet Drop Observed with Cisco PDSN

  A packet drop seen in Cisco PDSN is more than the allowed No Drop Rate (NDR) with maximum sessions.

  This condition occurs when a packet drop in the Cisco PDSN is more than the allowed 1 in 10,000 packets, when traffic is through the maximum number of sessions.

  Workaround: None.

Unresolved Caveats Cisco IOS Release 12.4(15)XR

The following caveats are unresolved in Cisco IOS Release 12.4(15)XR:

- CSCsu56357—[acct] G9 Wrongly Sent in Final Acct-Stop After RevA-RevA Handoff

On a Cisco router running Cisco IOS Release 12.4(15)XR, the G9 attribute value is incorrectly sent in an accounting record (accounting stop) for main flow on closing the session after RevA-RevA handoff.

This issue occurs after the following steps:

- A session is opened.
- RevA-RevA handoff is performed.
- The session is closed.

Workaround: None.

- CSCsu59055—**show cdma pdsn rp pcf stats** Shows Incorrectly

  The output for **show cdma pdsn rp pcf stats** shows incorrectly. Also the RP error statistics returned using the **rp error stats** command (such as Max Service Flows, Unsupported Service Option (SO), Non-Existent A10, and Bandwidth Unavailable) do not appear.

  This symptom is observed on a Cisco router that runs on Cisco IOS Release 12.4(15)XR on the Cisco PDSN 4.0 SAMI.

  Workaround: None.

- CSCsu62470—G9 Wrongly Sent in Acct-Stop to Old PCF after Dor-Act Handoff

  The G9 attribute value is incorrectly sent in accounting records (Acct-stop) of IP flows to the AAA server for old PCF after a Domant-Active Handoff. It should appear as “0” but it appears as “1”.

  This issue occurs after the following steps:

  - A session is opened.
  - The session is made dormant and the IP flows are inactivated by sending active stop fom PCF.
  - An active handoff is done.
  - The session is closed.

  Workaround: None.

Resolved Caveats

Resolved Caveats in Cisco IOS Release 12.4(15)XR10

- CSCtn95286— SAMI: Summit registers workaround for FRU power failure
- CSCtn83373—Cisco PDSN crashes with traceback cdma_sm_ipmobile_visitor_added_or_deleted.
- CSCto76913—Revocation does not workin PDSN Release r4.0.

Resolved Caveats in Cisco IOS Release 12.4(15)XR9

- CSCso28310—Memory leak occurs at rate_limit_insert, while unconfiguring access list with rate limit. The behavior occurs when access list is configured and then unconfigured.

Resolved Caveats in Cisco IOS Release 12.4(15)XR8

- CSCtc35874—Cisco PDSN may reload when the time-of-day accounting is configured.
- CSCtb61757—Cisco PDSN(LAC) may reload when session timeout is configured for VPDN calls.

- CSCsr89422—In Cisco PDSN Release 4.0, the PDSN application reloads at ipip_decaps and gre_ip_decaps.

Resolved Caveats in Cisco IOS Release 12.4(15)XR7

- CSCsz38104

  The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml.
- CSCtb04493—Debug condition causes continuous log related to mobile IP reverse-tunnel.
- CSCsz58449—PDSN may reload in case of mobile IP randomized IMSI scenario.
- CSCtb33607—PDSN may reload while closing the last session of a mobile IP tunnel.
- CSCtb25549—In Cisco PDSN Release 4.0, L2TP Access Controller (LAC) reboots when the VPDN conditional debugs are enabled.
- CSCta23040—In per-PCF-PPP statistics, the current connections counter shows a higher value compared to the global one.
- CSCtb41772—Empty or corrupt Mobile Directory Number (MDN) field in the Call Data Record (CDR) for handoff with PPP renegotiation.

Resolved Caveats in Cisco IOS Release 12.4(15)XR6

The following caveats are resolved in Cisco IOS 12.4(15)XR6:

- CSCta23281—Proxy mobile IP call does not work when the Cisco FA is configured for mobile IP solution with other vendors' HA.
- CSCsz91376—Proxy mobile IP does not work because of a false ARP entry that is created by proxy mobile IP on Cisco PDSN.
- CSCta15511—Unnecessary RADIUS debugs are displayed on console (one extra line for each MN call closure) when conditional debugs are enabled.
- CSCta23143—Airlink Active time is sent as zero during handoff.
- CSCta23040—In per-PCF-PPP statistics, the current connections counter shows a higher value compared to the global one.
- CSCsz86656—SAMI does not set the DBUS trust bit to one, which in turn causes the 7600 to re-mark the DSCP of the packets.
- CSCta15087—FA sends the Revocation Acknowledgement to port 434, instead of the source port.
- CSCsz74877—The CLI command **no ip mobile tunnel path-mtu-discovery** is lost after a reload.
- CSCta22610—During Proxy mobile IP call closure, FA sends a revocation message to the HA.
- CSCta49336—PPP options corrupted by Cisco PDSN relaying them to the LNS. This behavior is observed only for EVDO users.

Resolved Caveats in Cisco IOS Release 12.4(15)XR5

The following caveats are resolved in Cisco IOS 12.4(15)XR5:

- CSCsz21562—DSCP re-marking does not occur for main A10 EVDO calls in downstream.
- CSCsy92461—DSCP re-marking does not occur for main A10 of EVDO calls.
- CSCsz67185—A11 RRQ is rejected when both BSID and HRPD subnet elements are present.

Resolved Caveats in Cisco IOS Release 12.4(15)XR4

The following caveats are resolved in Cisco IOS 12.4(15)XR4:

- CSCta23228—Cisco PDSN reloads occasionally when deregistering a mobile IP flow.
- CSCsk41593—PAK_SUBBLOCK error found when packets are pinged with greater than 1500-byte over cellular interface.
- CSCsk64158—Cisco IOS software multiple features crafted UDP packet vulnerability.
- CSCsm27071—Cisco IOS software multiple features IP sockets vulnerability.
- CSCsm45113—RIB installs duplicate routes for the same prefix.
- CSCsm97220—Input queue blocked by MIPv6 packets.
- CSCsr29468—Cisco IOS software multiple features crafted TCP sequence vulnerability.
- CSCsw78831—(MIB) cCdmaFlowVpdnFailures always showing zero.
- CSCsw78901—The per-PCF counter shows wrong value.
- CSCsw79258—Cisco PDSN (LAC) fails to bring up the VPDN calls after stressing for long time.

Resolved Caveats in Cisco IOS Release 12.4(15)XR3

This caveat is resolved in Cisco IOS 12.4(15)XR3: CSCin61592—Allow Service Type=Authorize only for prepaid.

Resolved Caveats in Cisco IOS Release 12.4(15)XR2

The following caveats are resolved in Cisco IOS Release 12.4(15)XR2:

- CSCsu56357—G9 wrongly sent in final Acct-stop after Rev A-Rev A handoff.
- CSCsu59055—**show cdma pdsn rp pcf stats** showing incorrectly.
- CSCsu62470—G9 wrongly sent in Acct-stop to old PCF after Dor-Act handoff.
- CSCsu69297—Cisco PDSN reloads after Rev A-1x handoff.

Resolved Caveats Prior to Cisco IOS Release 12.4(15)XR1

There are no resolved caveats before Cisco IOS Release 12.4(15)XR1.

Related Documentation

Table 5 describes the related documentation that is available:

Table 5 Related Documentation

Document Title	Available Formats
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide, Release 12.4T	• On Cisco.com at http://www.cisco.com/en/US/docs/ios/mwpdsn/configuration/guide/12_4t/mwp_12_4t_book.html
Documentation on Cisco 7600 Router	• On Cisco.com at http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html
Documentation on Cisco Catalyst 6500 Switch	• On Cisco.com at http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
Documentation on Caveats for Cisco IOS Release 12.4	• On Cisco.com at http://www.cisco.com/en/US/products/ps6350/prod_release_notes_list.html

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.