Release Notes for the Cisco PDSN Feature in Cisco IOS Release 12.4(15)XR4

20 January 2009

Cisco IOS Release 12.4(15)XR4 is a special release that is based on Cisco IOS Release12.4, with the addition of enhancements to the Cisco Packet Data Serving Node (Cisco PDSN) feature. The Cisco IOS Release 12.4(15)XR4 is a release optimized for the Cisco PDSN feature on the Cisco Service and Application Module for IP (SAMI) Card on the Cisco 7609 Internet Router.

Contents

These release notes include important information and caveats for the Cisco PDSN software feature provided in Cisco IOS 12.4(15)XR4 for the Cisco 7609 Internet Router platform.

Caveats for Cisco IOS Release 12.4 can be found on CCO at:

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

Release notes for Cisco 7000 Family for Release 12.4T can be found on CCO at:

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

This release note includes the following topics:

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

© 2007 Cisco Systems, Inc. All rights reserved.

Introduction

Cisco PDSN is an IOS software feature that enables a Cisco Service and Application Module for IP (SAMI) on a Cisco 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 12.4(15)XR4:

Memory Requirements

Table 1 shows the memory requirements for the PDSN Software Feature Set that supports the SAMI card on the Cisco 7600 Internet router platform. The table also lists the memory requirements for the IP Standard Feature Set (for the Cisco PDSN).

Table 1 Memory Requirements for the SAMI Blade on the Cisco 7600 Router

Platform	Software Feature Set	Image Name	Flash Memory Required	DRAM Memory Required	Runs From
Cisco 7600 Internet Router	PDSN Software Feature Set	12.4(15)XR-c7svcsami-c6ik9s-mz.124-15.XR4 (This is a bundled image)	128MB	2048MB	RAM

Hardware Supported

Cisco IOS Release 12.4(15)XR4 is optimized for the SAMI Card on the Cisco 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/hwswmatrix.cgi

Software Compatibility

Cisco IOS Release 12.4(15)XR4 is a special release that is developed on Cisco IOS Release 12.4.

Cisco IOS Release 12.4(15)XR4 supports the same features that are in Cisco IOS Release 12.4, with the addition of the Cisco PDSN feature.

Migration Scenarios

The following table lists currently available or planned PDSN releases and the migration path to the SAMI platform:

Table 2 Migration Path for Cisco PDSN

	PDSN R3.0 or older	PDSN R3.5	PDSN R4.0
Platform	7200 NPE400/NPE-G1 and MWAM Platform (5 Processor only)	MWAM (5 Processor only)	Service Application Module for IP - SAMI
Chassis/Power Supply, Fan Trays)	7200VXR	6500/7600 Chassis	7600 Chassis
		SUP2/SUP720/	SUP720/RSP720/SUP 32
		SUP32SUP IOS **SX** based	**SUP IOS - SRC based image** (for example: c7600s72033-advipservicesk9-mz. 122-33.SRC.bin)
		SUP-redundancy	SUP-redundancy

Based on Table 2, there are many possible migration scenarios. In this document, we focus on those scenarios closest to current customer deployments. The actual migration path has to be determined per-customer end-to-end deployment. Additionally, migration should be engineered, and we recommend that you perform the migration in a maintenance window.

Customers may take this opportunity to redesign their network, for example, redesigning IP addresses scheme and configuring the routing protocols, network connectivity between PDSN and Home Agent, application connectivity between PDSN and AAA servers, routing on the new SAMI PDSN / Home Agent, etc.

Table 3 lists the most common migration scenarios:

Table 3 Migrations Scenarios for PDSN 4.0

Scenario	Migration From	To	Remarks
1	• Non-SR, • Non- Clustering, • 1- 7200VXR/NPE-G1 running PDSN	• Non-SR, • Non- Clustering, • 7600 Chassis, • One SUP720/SAMI (< 6 PPC) running PDSN	**Downtime:** Yes Other Comments: significant network provisioning changes in terms of, • Platform change • Configuration related to Platform (HW) • Configuration related to PDSN (SW) provisioning (Eg, Creation of Sub interfaces, VLAN, PCF secure configs etc). • 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 are planning to introduce additional features that are not enabled prior to migration.

Table 3 Migrations Scenarios for PDSN 4.0 (continued)

2	• Non-SR, • Non- Clustering, • Multiple 7200VXR/NPE-G1 running PDSN	• Non-SR, • Non-Clustering , • 7600 Chassis, • One SUP720/SAMI (all 6 PPC) running PDSN	**Downtime:** Yes Other Comments: Significant network provisioning change in terms of, • Platform change • New configuration related to Platform (SUP /SAMI) - (HW) • New configuration related to PDSN (SW) provisioning (Eg, Creation of Sub interfaces, VLAN, PCF secure configs etc). • 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 are planning to introduce additional features that are not enabled prior to migration.

Table 3 Migrations Scenarios for PDSN 4.0 (continued)

3	• Non-SR , • Non-Clustering • IPsec enabled between 7200 based PDSN and HA • Two-7200VXR/NPE-G1 running PDSN	• SR enabled, • Non-Clustering • 7600 Chassis, • SUP720 blade with redundancy • IOS based IPsec feature enabling • Two SAMI blades (Single chassis)	**Downtime:** Yes Other Comments: Significant network provisioning change in terms of, • Platform change • New Configuration related to Platform (SUP/SAMI) - (HW) • Crypto configuration to be done at Supervisor instead of PDSN processors. IPSec tunnel to be established between 7600 chassis running PDSN and HA application, instead of terminating the IPsec tunnels in PDSN/HA application itself (like that of 7200 platform). • New configuration related to PDSN (SW) provisioning (for example, creation of sub interfaces, VLAN, PCF secure configurations, etc.). • 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 are planning to introduce additional features that are not enabled prior to migration.

Table 3 Migrations Scenarios for PDSN 4.0 (continued)

4	• SR enabled, • Non-Clustering • 7600/Redundant SUP2 • Redundant MWAM blades (single chassis)	• SR enabled, • Non-Clustering • 7600/Redundant SUP 720 • Redundant SAMI blades (single chassis)	**Downtime:** Yes Other Comments: Minimal changes in terms of HW: • Upgrading platform (SUP 2 to SUP 720) – requires chassis reset. • New configuration related to SAMI Platform (HW) 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 are planning to introduce additional features that are not enabled prior to migration.
5	• SR enabled, • Non-Clustering • 7600/Redundant SUP 720 • Redundant MWAM blades(single chassis) • SUP IOS SXF	• SR enabled, • Non-Clustering • 7600/Redundant SUP 720 • Redundant SAMI blades(single chassis) • SUP IOS SRC	**Downtime:** Yes Other Comments: Minimal Changes in terms of HW: • Upgrading the SUP Image (SXF to SRC) requires chassis reset. • New configuration related to SAMI Platform (HW) 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 are planning to introduce additional features that are not enabled prior to migration.

Table 3 Migrations Scenarios for PDSN 4.0 (continued)

6	• SR enabled, • Non-Clustering • 7600/Redundant SUP 720 • Redundant MWAM blades (single chassis) • SUP IOS SXF	• SR enabled, • Clustering enabled, • 7600/Redundant SUP 720 • Redundant SAMI blades (single chassis) • SUP IOS SRC	**Downtime:** Yes Other Comments: Minimal Changes in terms of HW: • Upgrading the SUP Image (SXF to SRC) requires chassis reset. • New configuration related to SAMI Platform (HW) is enabled in SUP. • Configuration migration from MWAM processor to SAMI processor. • Provisioning of clustering setup requires introduction of clustering related configurations in PDSN processor, configuration of Controller, and configuration changes on the PCF side. **Note** We recommend that you allow the controller and member operate in different subnets. **Note** The majority of the basic configuration tasks related to the CDMA component remains the same, unless you are planning to introduce additional features that are not enabled prior to migration.

Table 3 Migrations Scenarios for PDSN 4.0 (continued)

7	• SR enabled, • Clustering enabled, • 7600/Redundant SUP 720 • Redundant MWAM blades (single chassis) • SUP IOS SXF	• SR enabled, • Clustering enabled, • 7600/Redundant SUP 720 • Redundant SAMI blades (dual chassis) • SUP IOS SRC	**Downtime:** Yes Other Comments: Significant changes in terms of HW: • Upgrading the SUP image (SXF to SRC) requires chassis reset. • Introduction of redundant chassis. • Provisioning the SUP configuration to operate in Inter- chassis redundancy environment. • New configuration related to SAMI platform (HW) is enabled in SUP. • Configuration migration from MWAM processor to SAMI processor. • Provisioning of clustering setup requires introducing clustering related configurations in the PDSN processor, configuration of controller, and configuration changes on the PCF side. **Note** The majority of the basic configuration tasks related to the CDMA component remains the same, unless you are planning to introduce additional features that are not enabled prior to migration.

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

Migration Steps

Migration to the Cisco PDSN R4.0 image is more than replacing MWAM modules with SAMI modules. Your migration should be well planned and conducted in a way that has minimal impact on the existing mobile subscriber's service connections.

Here are the migration tasks that are based on the scenarios that were previously established in Table 3.

Table 4 Migration Steps from PDSN 3.x to 4.0

Scenario	Migration Steps
1 , 2	• Install and configure PDSN on 7600/SUP720 (SRC based) with the SAMI. • Provision MS and PCFs to use the newly added SAMI-based PDSN (this may be a very large task). • Provision newly added PDSN with that of Home-agent to service Mobile IP calls. Also, modify the security association between PDSN and PCF's, PDSN and HA accordingly. • To minimize provisioning tasks, the SAMI PDSN instances can reuse the 7200 NPE-G1 based PDSN IP addresses and routing schemes (presuming this is done in a maintenance window, and that service will be disrupted).
3	• Install and configure the PDSN on 7600/SUP720 (SRC based) with the SAMI, and put them in the same HSRP redundancy group as configured on the Cisco 7200-based PDSN (R3.0 release). At this stage, the Cisco 7200-based PDSN will act as the active PDSN and the SAMI-based PDSN will assume the role of standby. • Ensure in the newly introduced SAMI based PDSN, that R3.5 or R4.0 features are not enabled. Also ensure that the features enabled on the SAMI PDSN are same as that of the features already enabled in 7200-based PDSN. However, the IPsec feature enabled onthe 7200 PDSN must be disabled on a SAMI-based PDSN. Instead, the IPsec configuration will be moved to the 7600 Supervisor configuration, and the IPsec tunnel will be established between the chassis. Once the packet is taken out of the IPsec tunnel in the supervisor, the same is sent to the PDSN instances through the backplane. • Configure higher priority and HSRP preemption (with delay) on the SAMI-based PDSN. • Let the SAMI PDSN takes over the active role. • Bring down the Cisco 7200s and introduce another SAMI card (SAMI card 2) in the same chassis, and configure the redundancy. Let the SAMI card 2, takes over the role of standby PDSN. – 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, the above mentioned step does not need to be performed in a maintenance window. – However, introduction of new features (such as R4.0) should be done during a maintenance window.

Table 4 Migration Steps from PDSN 3.x to 4.0

4	• Install and configure PDSN on 7600/SUP720 (SRC based) with SAMI and put them in the same HSRP redundancy group as configured on MWAM-based PDSN (R3.0 release). At this stage, the MWAM PDSN instances will act as the active PDSN and the SAMI-based PDSN will assume the role of standby. **Note** The SAMI card can be configured for 6 instances of PDSN, whereas the MWAM will have only 5 instances. Customers can efficiently provision the network and distribute the load across 6 PDSN instances (instead of 5) during the upgrade process. • Configure SUP720 to support SAMI. – Make sure MWAM configurations are saved on SUP720 bootflash. – Configure the VLAN for SAMI VLAN groups on SUP720 as MWAM. – Build SAMI PPC configuration from MWAM processors configurations according to SAMI configuration file name convention in SUP720 bootflash. – Power down the standby MWAM and pull it out of the chassis. – Insert the SAMI in the same slot and boot it with the proper PDSN R4.0 image. – Verify SAMI PPC gets the proper PDSN configurations. • Ensure, the newly introduced SAMI-based PDSN does not enable any of the R3.5 or R4.0 features. Also ensure that the features enabled on the SAMI PDSN are the same as that of the features already enabled on the MWAM-based PDSN. • Configure higher priority and HSRP preemption (with delay) on SAMI based PDSN. • Let the SAMI PDSN takes over active role. • Bring down the standby MWAM and introduce another SAMI card (SAMI card 2) in the same chassis, and configure the redundancy. Let the SAMI card 2, takes over the role of standby PDSN. – 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, the above mentioned step does not need to be performed in a maintenance window. • However, introducing new features (such as R4.0) should be done 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 will be reset, too. Same is the case for Sup2 to Sup 720 or Sup 32 or RSP 720 migration. • This should be performed in a maintenance window. • User service will be disrupted. • For MWAM to SAMI PDSN migration, follow the steps given in Scenario 4.

Table 4 Migration Steps from PDSN 3.x to 4.0

6	• Since the SAMI blade does not support Inter-PPC communication on a same Vlan , the existing cluster-member architecture model of the PDSN on a single MWAM blade requires few configuration changes during provisioning using the SAMI platform (out of 5 processors in the MWAM, 1 is used as controller and rest of the processors are used as a PDSN member).You need to use the ip-address from different subnet on the controller and member interface, and enable explicit routing through the supervisor in order for them to communicate with each other. **Note** This would call for additional configuration (i.e., change in Cluster controller IP address in PCF, routing, etc.) on the PCF side as well. • Additionally, the cluster related configuration has to be newly introduced in PDSN member in order for the member to participate in a cluster environment. • The remaining migration steps are similar to Scenario 4 and 5. • The above migration must be performed in maintenance window.
7	• The migration steps are very similar to scenario 5. **Note** It is not recommended to have MWAM (R3.0 image) and SAMI PDSN (R4.0 image) members participating in same cluster controller based on R3.0 image, the reason being, • Handling of Rev. A calls: we need to enable the CLI to support multiple flows which cannot be done in R3.0 based controller. • Additionally, having a SAMI and an MWAM PDSN participating in a single controller might end up re-directing / suggesting MWAM R3.0 PDSN IP address for a Rev. A call.

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 IOS Software, MWAM Software (MWAM-C6IS-M), Version 12.4(15)XN , RELEASE SOFTWARE
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 11-Dec-07 15:44 by jsomiram

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

PDSN-S2000-BAL uptime is 4 minutes
System returned to ROM by bus error at PC 0x2033D804, address 0x283 at 06:56:44 PDT Mon
Dec 3 2007
System restarted at 03:29:24 PDT Tue Dec 11 2007
System image file is "svcmwam-c6is-mz.xn"

Cisco MWAM (MWAM) processor with 997376K/32768K bytes of memory.
SB-1 CPU at 700MHz, Implementation 1025, Rev 0.2

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

Configuration register is 0x4

Router#
```

Upgrading to a New Software Release

The following sections contain details on how to upgrade your Cisco PDSN:

- Upgrading the Supervisor Image
- Upgrading the SAMI Software
- Changing Configuration on the PDSN in a Live Network

Upgrading the Supervisor Image

To upgrade the Supervisor image, perform the following procedure:

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

Step 2 Add the following command to the running config boot system disk0: *SUP image name*. Here is an example:

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

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

Step 3 Perform a "write memory" so that running configuration is saved on both active and standby SUP.

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

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

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

Upgrading the SAMI Software

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

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

Changing Configuration on the PDSN in a Live Network

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

Step 1 Bring the standby PDSN out of service. An example would be to unconfigure the **cdma pdsn redundancy** command on the standby PDSN. This isolates the standby PDSN from the session redundancy setup.

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

Step 2 Perform a "write memory" so that running configuration is saved.

Step 3 Now make the necessary configuration changes on the standby PDSN, and save the configuration.

Step 4 Re-configure the **cdma pdsn redundancy** command, and save the configuration.

Step 5 Issue the **reload** command to bring the standby PDSN back into the session redundancy setup with the changed configuration. Verify the processor comes back in the SR setup using the following show commands:

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

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

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

CDMA PDSN Session Redundancy Statistics
  Last clearing of cumulative counters never
                      Total              Current
                Synced from active      Connected
  Sessions                15                   15
  SIP Flows               15                   15
  MIP Flows               0                    0
PMIP Flows               0                    0

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

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

     Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up

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

7600a-Stdy#
```

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

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

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

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

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

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

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

MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 5.

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 12.4(15)XR4 supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(15)XR4 includes the PDSN feature. The Cisco IOS Release 12.4(15)XR4 is a release optimized for the Cisco PDSN feature on the Cisco Service and Application Module for IP (SAMI) Card on the Cisco 7609 Internet 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 12.4(15)XR4

The Cisco IOS Release 12.4(15)XR4 supports the same feature sets as Cisco Release 12.4, with the exception that Cisco Release 12.4(15)XR4 includes the PDSN feature. The Cisco PDSN feature is optimized for the Cisco SAMI card on the Cisco 7600 Internet router, and includes the following new and existing features:

- Attribute Support
- Served MDN
- Framed Pool
- 3GPP2 DNS Server IP
- Virtual Route Forwarding (VRF) with Sub-interfaces 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
- CAC
- Home Area, Maximum Authorized Aggregate Bandwidth and Inter-user Priority Attributes Downloaded from AAA
- Support for Mobile Equipment Identifer (MEID)
- Simple IPv6 Access
- Session Redundancy Infrastructure
- Radius Server Load Balancing

- Closed-RP/Open-RP Integration
- Subscriber Authorization Based on Domain
- PPP Counters
- RP Counters
- Conditional Debugging Enhancements
- Trace Functionality
- Mobile IP Dynamic Home Address Deletes Older Sessions With Different IMSI
- Protocol Layering and RP Connections
- PPPoGRE RP Interface
- A11 Session Update
- SDB Indicator Marking
- Resource Revocation for Mobile IP
- Packet of Disconnect
- IS-835 Prepaid Support
- Prepaid Billing
- Mobile IP Call Processing Per Second Improvements
- IS-835-B Compliant Static IPSec
- Always On Feature
- 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

Caveats

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

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

The "Open Caveats" section lists open caveats that apply to the current release and might also apply to previous releases.

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

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

Open Caveats

There are no new unresolved caveats in Cisco IOS Release 12.4(15)XR4.

Unresolved Caveats Prior to Cisco IOS Release 12.4(15)XR4

There are no new unresolved caveats in Cisco IOS Release 12.4(15)XR3.

Unresolved Caveats Prior to Cisco IOS Release 12.4(15)XR3

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

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

  For MIP calls G15 and G16 for IP flows are incorrectly sent. When session is closed for IP flows, G15 & G16 sending the same values as the session.

  This issue is seen under the following conditions:

  - Open a MIP session with forward and reverse ipflows.
  - Install TFT with forward and reverse packet filters (for opened ipflows).
  - Close the session.

  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 f14 are sent as non-zero values in acct-records for the new PCF.

  This issue occurs under the following conditions:

  - Open a session.
  - Make it dormant by sending active stop from pcf.
  - Perform a dormant-dormant handoff

  Workaround: none.

Unresolved Caveats Prior to Cisco IOS Release 12.4(15)XR2

The following caveats are unresolved in Cisco IOS Release 12.4(15)XR1:

- CSCsu89978—Packet Drop Observed with PDSN

  A packet drop seen in PDSN is more than the allowed NDR rate with maximum sessions .

  This condition occurs when a packet drop in the PDSN is more than the allowed 1 in 10000 packets, when traffic is through maximum number of sessions.

  Workaround: none.

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

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

  This issue occurs under the following conditions:

  - Opened a session.
  - Performed RevA-RevA handoff.
  - Closed the session.

  Workaround: none.

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

  show cdma pdsn rp pcf stats are showing incorrectly and the **rp error stats** (Max Service Flows , Unsupported So, Non-Existent A10, Bandwidth Unavailable) not showing in rp pcf stats.

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

  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 AAA for old PCF after a Domant-Active Handoff. It should appear as “0” but it is appearing as “1”.

  This symptom occurs under the following conditions:

  - Opened a session.
  - Made the session dormant and ipflows inactive by sending active stop fom pcf.
  - Then did an active handoff.
  - Closed the session.

  Workaround: none.

Resolved Caveats

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

- CSCsk41593—PAK_SUBBLOCK Error Found When Ping with >1500-byte Over Cellular Inter

  The following error occurs when a ping packet is sent or received:

  ```
  PAK_SUBBLOCK_ALREADY: 2 -Process= "IP Input"
  ```

  This condition occurs when large ping packets (greater than 1500 bytes) are sent to back-to-back cellular interfaces with GRE tunneling enabled.

  Workaround: Disable the **ip virtual-reassembly** command on the cellular interface.

- CSCsk64158

  Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml.

- CSCsm27071

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

- CSCsm45113—RIB Installs Duplicate Routes for the Same Prefix

  The router may install duplicate routes or incorrect route netmask into routing table. It could happen on any routing protocol. Additionally, for OSPF, a reload was observed.

  The problem is triggered by SNMP polling of ipRouteTable MIB. The problem is introduced by CSCsj50773, see the Integrated-in field of CSCsj50773 for affected images.

  Workaround: do not poll the ipRouteTable MIB, instead poll the newer replacement ipForward MIB. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

  The **clear ip route** command can correct the routing table until the next poll of ipRouteTable MIB.

- CSCsm97220

  Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at the following link
  http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml

- CSCsr29468

  Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

- CSCsw78831—[MIB] cCdmaFlowVpdnFailures Always Showing Zero

  On a Cisco router running the PDSN 4.0 software, the MIB cCdmaFlowVpdnFailures always shows zero (0).

  This occurs under normal failure conditions.

  Workaround: none.

- CSCsw78901—Per PCF counter is Showing Wrong Value

  On a Cisco router running PDSN 4.0 software, per PCF current connections under the **show cdma pdsn statistics ppp pcf** command are larger than the actual current connections in the PDSN.

  Additionally, we observed that the connection req field in the **show cdma pdsn stat ppp pcf** command is unreasonably large.

  The first condition occurs when the Service Option is sent after A10 establishment.

  The second conditions occurs when the Service Option is sent during PPP negotiation and the **cdma pdsn mib ignore mn-failures no-lcp-confreq** command is configured.

  Workaround: there is no workaround for the first condition. To work around the second condition, remove the **cdma pdsn mib ignore mn-failures no-lcp-confreq** command.

- CSCsw79258—PDSN (LAC) Fails to Bring up the VPDN Calls After Stressing For Long Time

  On a Cisco router running PDSN 4.0 software, the PDSN fails to bring up VPDN calls after stressing for long time.

  This condition occurs when a large number of VPDN subscribers fail to establish calls, and if they continue retrying (for example, AAA not reachable, LNS not reachable, network outage, etc.), the PDSN per session IDs may exhaust after some time. After reaching this stage, the PDSN will not accept any new VPDN calls.

  Workaround: none.

Resolved Caveats Prior to Cisco IOS Release 12.4(15)XR4

The following caveats are resolved in Cisco IOS 12.4(15)XR3:

- CSCin61592—Allow Service Type=Authorize Only for Prepaid

  Allow Service Type=Authorize Only for Prepaid and also includes the Framed IP address in an online Access request.

  a. Open a session with Prepaid accounting enabled.
  b. Send traffic till quoata reached, then PDSN will send Online Access request to AAA with service-type set to Outbound for additional quota.
  c. AAA will send Access reject to PDSN.

  Workaround: none.

Resolved Caveats Prior to Cisco IOS Release 12.4(15)XR3

The following caveats are resolved in Cisco IOS Release 12.4(15)XR1:

- CSCsu56357—G9 Wrongly Sent in Final Acct-stop After Reva-Reva Handoff

  On Cisco router running Version 12.4(15)XR, the G9 attribute value wrongly sent in accounting record (accounting stop) for main flow upon closing the session after RevA-RevA handoff.

  The following conditions exist:

  - Opened a session
  - Performed RevA-RevA handoff
  - Closed the session.

  Workaround: none.

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

  The **show cdma pdsn rp pcf stats** command displays incorrectly, and **rp error stats** (Max Service Flows, Unsupported So, Non-Existent A10, Bandwidth Unavailable) are not showing in **rp pcf** stats.

  This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4 (15)XR on SAMI 4.0 PDSN image

  Workaround: none.

- CSCsu62470—G9 Wrongly Sent In Acct-stop to Old Pcf After Dor-Act Handoff

  The G9 attribute value is mistakenly sent in accounting records (Acct-stop) of IP-flows to AAA for old PCF after a domant-active handoff. The value should be sent as “0” but is going as “1”.

  The following conditions exist:

  - Opened a session.
  - Made the session dormant and ipflows inactive by sending active stop fom pcf.
  - Performed an active handoff.
  - Closed the session.

  Workaround: none.

- CSCsu69297—PDSN Reloads After Reva-1x Handoff

  After RevA-1x handoff, the PDSN reloaded.

  This issue occurs under the following conditions:

  - Open a Rev-a session.
  - Install Packet filters.
  - Perform handoff to 1x.

  Workaround: none.

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

There were no resolved caveats prior to Cisco IOS Release 12.4(15)XR1.

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 24
- Platform-Specific Documents, page 24

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.4T:

- *Packet Data Serving Node (PDSN) Release 3.5* at the following url:

  http://www.cisco.com/en/US/products/ps6706/products_feature_guides_list.html

Platform-Specific Documents

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

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

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

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2009, Cisco Systems, Inc.
All rights reserved.