



Release Notes for Cisco PDSN Release 5.0 in IOS Release 12.4(22)XR

Published: August 21, 2009

Revised: September 24, 2009, OL-19028-01

Cisco IOS Release 12.4(22)XR is based on Cisco IOS Release 12.4, with enhancements to the Cisco Packet Data Serving Node (Cisco PDSN) feature. This Cisco PDSN Release 5.0 based on IOS Release 12.4 is optimized for the Cisco PDSN feature on the Cisco Service and Application Module for IP (SAMI) card on the Cisco 7600 Series Router.

Contents

These release notes include important information and caveats for the Cisco PDSN software feature provided by the Cisco IOS 12.4(22)XR for the Cisco 7600 Series Router platform.

This release note describes:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Migration to Cisco PDSN, page 4](#)
- [Upgrading to New Software Release, page 12](#)
- [Cisco PDSN Software Features in Release 12.4\(22\)XR, page 16](#)
- [Caveats, page 18](#)
- [Related Documentation, page 24](#)
- [Obtaining Documentation and Submitting a Service Request, page 25](#)



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(22)XR:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 2](#)
- [Software Compatibility, page 3](#)
- [Cisco PDSN Software Features in Release 12.4\(22\)XR, page 16](#)

Memory Requirements

To install Cisco PDSN software that supports the SAMI card on the Cisco 7600 Series Router:

- Platform: Cisco 7600 Series Router
- Software/Feature Set: PDSN Software Feature Set
- Image Name: *12.4(22)XR – c7svcsami-c6ik9s-mz.124.22.XR* (This file is a bundled image file)
- Required Flash Memory: 256 MB
- Required DRAM Memory: 2048 MB
- Runs From: RAM

Hardware Supported

Cisco IOS Release 12.4(22)XR 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 login to this tool:

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

Software Compatibility

Cisco IOS Release 12.4(22)XR is developed on Cisco IOS Release 12.4 and supports the features included in Cisco IOS Release 12.4, 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\(22\)XR](#).

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
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 5.0:

- [Migration Path for Cisco PDSN, page 4](#)
- [Migration Scenarios for Cisco PDSN 5.0, page 5](#)
- [Migration Steps, page 8](#)

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*

	Cisco PDSN Release 3.0 or earlier	Cisco PDSN Release 3.5	Cisco PDSN Release 4.0	Cisco PDSN Release 5.0
Platform	7200 NPE400/NPE-G1 and MWAM platform (5 processor only)	MWAM (5 processor only)	SAMI	SAMI
Chassis/Power Supply, Fan Trays)	7200VXR	6500/7600 chassis	7600 chassis	7600 chassis
—	—	SUP2/SUP720	SUP720/RSP720/SUP 32	SUP720
—	—	SUP32/SUP IOS SX based	SUP IOS - SRC-based image (for example: <i>c7600s72033-advipservicesk9-mz.122-33.SRC.bin</i>)	SUP IOS - Latest SRC-based image
—	—	SUP redundancy	SUP redundancy	SUP redundancy

Migration Scenarios for Cisco PDSN 5.0

Based on [Table 2](#), there are many possible migration scenarios. This section focuses on those scenarios 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 HA.
 - Configuring application connectivity between Cisco PDSN and AAA servers.
 - Configuring routing on the new SAMI Cisco PDSN or the HA.


Note

For all 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.

[Table 3](#) lists the most common migration scenarios.

Table 3 *Migrations Scenarios for Cisco PDSN Release 5.0*

Scenario	Migration From	To	Remarks	Downtime
1	<ul style="list-style-type: none"> • Non-SR • Non- clustering • 7600 chassis • Each processor can act as an individual Cisco PDSN 	<ul style="list-style-type: none"> • Non-SR • Non- clustering • 7600 chassis • One Cisco PDSN per blade (single IP architecture) 	<ul style="list-style-type: none"> • Erase existing configuration in all processors. • After upgrading to Cisco PDSN Release 5.0, ensure that the configuration is done only on the PCOP (that is, processor 3). • IP address-pool requirements in Cisco PDSN Release 5.0 (at blade level) are five times that configured in Cisco PDSN Release 4.0 (at processor level). 	Yes

Table 3 *Migrations Scenarios for Cisco PDSN Release 5.0 (continued)*

2	<ul style="list-style-type: none"> • Non-SR • Non-clustering • 7600 chassis • One blade with each processor acting as an individual Cisco PDSN 	<ul style="list-style-type: none"> • SR enabled • Non-clustering • 7600 chassis • Two SAMI blades (in the same chassis) with a single Cisco PDSN at the blade level • Auto synchronization enabled 	<ul style="list-style-type: none"> • Erase existing configuration in all processors on active and standby blades. • After upgrading to Cisco PDSN Release 5.0, ensure that the configuration is done only on an active blade PCOP (that is, processor 3). • Ensure that the standby SAMI blade is shutdown while configuring the active. • IP address-pool requirements in Cisco PDSN Release 5.0 (at blade level) are five times that configured in Cisco PDSN Release 4.0 (at processor level). 	Yes
3	<ul style="list-style-type: none"> • SR-enabled • Non-clustering • 7600 chassis • Two SAMI blades (in the same chassis) 	<ul style="list-style-type: none"> • SR-enabled • Non-clustering • 7600 chassis • Two SAMI blades (in the same chassis) • Auto synchronization enabled 	<ul style="list-style-type: none"> • Erase existing configuration in all processors on active and standby blades. • After upgrading to Cisco PDSN Release 5.0, ensure that the configuration is done only on an active blade PCOP (that is, processor 3). • Ensure that the standby SAMI blade is shutdown while configuring the active. • IP address-pool requirements in Cisco PDSN Release 5.0 (at blade level) are five times that configured in Cisco PDSN Release 4.0 (at processor level). 	Yes
4	<ul style="list-style-type: none"> • Non-SR • Clustering enabled • 7600 chassis • One or more processors running a Cisco PDSN member 	<ul style="list-style-type: none"> • Non-SR • Clustering enabled • 7600 chassis • One Cisco PDSN member per blade 	<ul style="list-style-type: none"> • Erase existing configuration in all processors on active and standby blades. • After upgrading to Cisco PDSN Release 5.0, ensure that the configuration is done only on an active blade PCOP (that is, processor 3). • IP address-pool requirements in Cisco PDSN Release 5.0 (at blade level) are five times that configured in Cisco PDSN Release 4.0 (at processor level). 	Yes

Table 3 *Migrations Scenarios for Cisco PDSN Release 5.0 (continued)*

5	<ul style="list-style-type: none"> • SR enabled (controller redundancy) • Clustering enabled • 7600 chassis • Running controller in one of the processors • Redundant SAMI blades (in the same chassis) 	<ul style="list-style-type: none"> • SR enabled • Clustering enabled • 7600 chassis • Can run both controller and collocated member • Redundant SAMI blades (in the same chassis) • Auto synchronization enabled 	<ul style="list-style-type: none"> • Erase existing configuration in all processors on active and standby blades. • After upgrading to Cisco PDSN Release 5.0, ensure that the configuration is done only on an active blade PCOP (that is, processor 3). • Ensure that the standby SAMI blade is shutdown while configuring the active. • If collocated member is configured, ensure that session redundancy is enabled. • IP address-pool requirements in Cisco PDSN Release 5.0 (at blade level) are five times that configured in Cisco PDSN Release 4.0 (at processor level). 	Yes
6	<ul style="list-style-type: none"> • SR-enabled • Clustering-enabled • 7600 Chassis • Redundant SAMI blades (in the dual chassis) 	<ul style="list-style-type: none"> • SR-enabled • Clustering-enabled • 7600 Chassis • Redundant SAMI blades (in the inter chassis) • Auto synchronization disabled (default) 	<ul style="list-style-type: none"> • Erase existing configuration in all processors on active and standby blades. • After upgrading to Cisco PDSN Release 5.0, ensure that the configuration is done only on an active blade PCOP (that is, processor 3). • If configured, Cisco PDSN acts as controller and collocated member. • IP address-pool requirements in Cisco PDSN Release 5.0 (at blade level) are five times that configured in Cisco PDSN Release 4.0 (at processor level). 	Yes

Migration Steps

Migration to the Cisco PDSN Release 5.0 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 Table 3.

Table 4 *Migration Steps from Cisco PDSN 4.0 to 5.0*


Scenario	Migration Steps
1	<ul style="list-style-type: none"> • In SAMI cards with Cisco PDSN Release 4.0, erase configuration on all processors and reload Cisco PDSN. • Configure the I/O memory (IOMEM) on all processors as 256 MB and save the configuration to the NVRAM. <div>  Note If you have set the IOMEM size as 64 MB, ensure that you configure the memory lite command. The recommended memory size is, however, 256 MB. </div> <ul style="list-style-type: none"> • Upgrade to Cisco PDSN Release 5.0 and reconfigure the Cisco PDSN configuration on processor 3. • Provision MS and PCFs to use the newly added Cisco PDSN Release 5.0-based PDSN IP. • Provision the newly added PDSN with the HA to service MIP calls. <p>To minimize provisioning tasks, Cisco PDSN Release 5.0 reuses the IP address and routing scheme used in one of the Cisco PDSN Release 4.0 processors.</p> <p>1. MS = Mobile Station. 2. PCF = Packet Control Function.</p>

Table 4

Migration Steps from Cisco PDSN 4.0 to 5.0 (continued)


2, 3	<ul style="list-style-type: none"> • Install the new SAMI card on 7600/720 that is to be used in redundant configuration. • In the existing Cisco PDSN Release 4.0, erase the existing configuration on all processors and reload the Cisco PDSN. • Configure the IOMEM size on all processors as 256 MB and save the configuration to the NVRAM. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <p>Note If you have set the IOMEM size as 64 MB, ensure that you configure the memory lite command. The recommended memory size is, however, 256 MB.</p> </div> <ul style="list-style-type: none"> • Upgrade both the SAMI blades to Cisco PDSN Release 5.0. • Shut down the blade for configuration as standby (unit2). • Enable auto synchronization on the active blade (unit1). Configure the PDSN on active blade on processor 3. Keep unit2 as a standby in a redundant configuration. When configuring redundancy, you must configure Hot Standby Router Protocol (HSRP) main interface before configuring Interprocessor Communication (IPC). • Save the configuration on the active blade. • Bring up unit2 with Cisco PDSN Release 5.0 image. Configurations are auto synchronized from the active blade. • Verify the output of the show redundancy state and show redundancy inter device commands on both active and standby blades to confirm if redundancy is enabled. If the output for one of the blades requires a reload to enable redundancy, reload that blade. • Provision MS and PCFs to use the newly added Cisco PDSN Release 5.0-based PDSN IP. • Use the CDMA-1x IP address on the PDSN as controller or member IP when provisioning. • Provision the newly added PDSN with that of HA to service MIP calls. <p>To minimize provisioning tasks, Cisco PDSN Release 5.0 reuses the IP address and routing scheme used in one of the Cisco PDSN Release 4.0 processors.</p>
------	---

Table 4 **Migration Steps from Cisco PDSN 4.0 to 5.0 (continued)**


4	<ul style="list-style-type: none"> • In SAMI cards with Cisco PDSN Release 4.0, erase the existing configuration on all processors and reload Cisco PDSN. If the blade includes Cisco PDSN members as part of the cluster, we recommend that you remove the PDSN member part before reloading. • Configure the IOMEM size on all processors as 256 MB and save the configuration to the NVRAM. <div data-bbox="467 436 509 470"></div> <div data-bbox="467 478 1468 541"> <p>Note If you have set the IOMEM size as 64 MB, ensure that you configure the memory lite command. The recommended memory size is, however, 256 MB.</p> </div> <ul style="list-style-type: none"> • Upgrade to Cisco PDSN Release 5.0 and reconfigure the PDSN on processor 3. • You can configure the Cisco PDSN as both controller and collocated member. Cisco PDSN Release 5.0 interoperates with Cisco PDSN Release 3.0 or 4.0 controller or member. • Provision MS and PCFs to use the newly added Cisco PDSN Release 5.0-based PDSN IP. • Use the CDMA-1x IP address on the PDSN as controller or member IP when provisioning. • Provision newly added PDSN with that of HA to service MIP calls. <p>To minimize provisioning tasks, Cisco PDSN Release 5.0 reuses the IP address and routing scheme used in one of the Cisco PDSN Release 4.0 processors.</p>
---	---

Table 4

Migration Steps from Cisco PDSN 4.0 to 5.0 (continued)



5	<ul style="list-style-type: none"> • Install the new SAMI card on 7600/720 that is to be used in redundant configuration. • In the existing Cisco PDSN Release 4.0, erase the existing configuration on all processors and reload the Cisco PDSN. • Configure the IOMEM size on all processors as 256 MB and save the configuration to the NVRAM. <div data-bbox="505 443 548 485"></div> <div data-bbox="500 489 1518 556"> <p>Note If you have set the IOMEM size as 64 MB, ensure that you configure the memory lite command. The recommended memory size is, however, 256 MB.</p> </div> <ul style="list-style-type: none"> • Upgrade both the SAMI blades to Cisco PDSN Release 5.0. • Shut down the blade for configuration as standby (unit2). • Enable auto synchronization on the active blade (unit1). Configure the PDSN on active blade on processor 3. Keep unit2 as a standby in a redundant configuration. When configuring redundancy, you must configure Hot Standby Router Protocol (HSRP) main interface before configuring Interprocessor Communication (IPC). • Save the configuration on the active blade. • Bring up unit2 with Cisco PDSN Release 5.0 image. Configurations are auto synchronized from the active blade. • Verify the output of the show redundancy state and show redundancy inter device commands on both active and standby blades to confirm if redundancy is enabled. If the output for one of the blades requires a reload to enable redundancy, reload that blade. • Provision MS and PCFs to use the newly added Cisco PDSN Release 5.0-based PDSN IP. • Use the CDMA-1x IP address on the PDSN as controller or member IP when provisioning. • Provision the newly added PDSN with that of HA to service MIP calls. • You can configure the Cisco PDSN to act as controller and collocated member. <ul style="list-style-type: none"> – In the case of a collocated member, ensure that you enable session redundancy, so that the standby is synchronized with sessions handled by the collocated member. – For an active controller to synchronize the information with the standby controller, ensure that all remote members connect to the HSRP main interface of the controller. – If the member IP is configured, ensure that it is the same as the CDMA -1x interface IP address.
---	--

Table 4

Migration Steps from Cisco PDSN 4.0 to 5.0 (continued)

6	<ul style="list-style-type: none"> • In the existing Cisco PDSN Release 4.0, erase the existing configuration on all processors and reload the Cisco PDSN. • Configure the IOMEM size on all processors to 256 MB and save the configuration to the NVRAM. <div>  <p>Note If you have set the IOMEM size as 64 MB, ensure that you configure the memory lite command. The recommended memory size is, however, 256 MB.</p> </div> <ul style="list-style-type: none"> • Upgrade both the SAMI blades to Cisco PDSN release 5.0. • Reconfigure the Cisco PDSN and enable inter-chassis HSRP redundancy as in Cisco PDSN release 4.0. • Provision MS and PCFs to use the newly added Cisco PDSN Release 5.0-based PDSN IP. • Use the CDMA-1x IP address on the PDSN as controller or member IP when provisioning. • Provision the newly added Cisco PDSN with the HA to service MIP calls.
---	---

Upgrading to New Software Release

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

- [Determining the Software Version, page 13](#)
- [Upgrading the Supervisor Image, page 14](#)
- [Upgrading the SAMI Software, page 14](#)
- [Changing Configuration on Cisco PDSN in a Live Network, page 14](#)

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

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](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 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 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 PDSN back into the session redundancy setup with the changed configuration. Verify if 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-srl 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 PDSN to take over as active by reloading the current active 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 synched with new active units.

Step 7 Configure the current standby PDSN using the procedures described from [Step 1](#) to [Step 5](#).



Note

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

Cisco PDSN Software Features in Release 12.4(22)XR

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 because of 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.

Cisco IOS Release 12.4(22)XR supports the same feature sets as Cisco Release 12.4; additionally, it supports the PDSN feature. Cisco PDSN Release 5.0 includes the following new and existing features:

- Single IP per Blade
- Osler Support
- Improved Throughput and Transaction Handling
- Cluster Controller Support in Single IP Blade
- IMSI and PCF Redirection
- Mobile IP and AAA Attributes for China Telecom
- Trap Generation for AAA Server Unresponsiveness
- Supervisor Support
- Data Over Signaling
- Differentiated Services Code Point Marking Support
- Nortel Aux A10 Support
- Masking Off IMSI Prefix
- Persistent TFT Support
- Conserve Unique IP-ID for FA-HA IP-in-IP Tunnel
- GRE CVSE Support in FA-HA Tunnel
- Remote Address Accounting
- Default Service Option Implementation
- Configurable Per-Flow Accounting Options
- IP Flow Discriminator Support for PCF Backward Compatibility
- Support for Remark DSCP to Max-class Value
- Command Support for Fragmentation Size
- New Statistics Counters for China Telecom
- Attribute Support
 - Served MDN
 - Framed Pool

- 3GPP2 DNS Server IP
- Virtual Route Forwarding with Sub-interfaces
- Conditional Debugging Enhancements (for Cisco PDSN Release 4.1)
- Multiple Service Connections
- Data Plane
- Subscriber QoS Policy (both downloading per-user profile from the AAA server and configuring a local profile)
- QoS Signaling
- Traffic Flow Templates
- Per-flow Accounting
- Call Admission Control
- PDSN MIB Enhancements (for Cisco PDSN Release 4.0)
- PDSN on SAMI
- Inter-User Priority
- Roamer Identification
- Bandwidth Policing
- Packet Data Service Access—Simple IPv6 Access
- Session Redundancy Infrastructure
- RADIUS Server Load Balancing
- Subscriber Authorization Based on Domain
- PDSN MIB Enhancements
 - PPP Counters in Cisco PDSN Release 3.0
 - RP Counters in Cisco PDSN Release 3.0
- Conditional Debugging Enhancements—Trace Functionality in Cisco PDSN Release 3.0
- Randomized IMSI Handling
- 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
- Always-On Feature
- PDSN MIB Enhancements
- Conditional Debugging Enhancements
- Cisco Proprietary Prepaid Billing

- 3DES Encryption
- Mobile IP IPSec
- Hardware IPSec Acceleration Using IPSec Acceleration Module—Static IPSec
- 1xEV-DO Support
- Integrated Foreign Agent
- AAA Server Support
- Packet Transport for VPDN
- Proxy Mobile IP
- Multiple Mobile IP Flows
- PDSN Cluster Controller / Member Architecture

Refer the *Cisco Packet Data Serving Node Release 5.0 for Cisco IOS Release 12.4(22)XR* for more information on the features.

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 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 may also apply to previous releases.

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

The “[Product Documentation](#)” 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

The following are the unresolved caveats in Cisco IOS Release 12.4(22)XR and earlier releases.

Unresolved Caveats in Cisco IOS Release 12.4(22)XR

- CSCtb30757—RAA Flow Count Does Not Get Cleared in Standby Mode.

The RAA flow count does not get cleared in the standby mode. When a high number of sessions are opened, the flow counts are displayed correctly. When the sessions are closed or cleared, the flow counts are cleared in the active mode; but they still appear in the standby mode.

This issue is seen:

- when flapping simple IP (SIP) and mobile IP (MIP) sessions.

Workaround: None.

- CSCtb49920—Prepaid Per PCF Statistics Counter Displays The Wrong Output When Doing Handoff With PPP Renegotiation.

When doing inter pcf handoff with ppp renegotiation for the prepaid session, the client service termination and total online access requests sent counters are showing wrongly in new pcf instead of old pcf under **show cdma pdsn statistics prepaid pcf ip addr**.

This issue is seen:

- when a prepaid session is opened.
- when inter pcf handoff is performed with ppp renegotiation.

Workaround: None.

- CSCtb43404—Mobile IP Tunnel Information Does Not Get Cleared in Standby Mode.

In a standby Cisco PDSN, tunnel user counters in **show ipmobile tunnel** appear differently from an active PDSN.

This issue is seen:

- With MIP sessions:
 - Open 100 MIP sessions , tunnel users counters match in both active and standby Cisco PDSNs, reflecting the number of users connected.
 - Perform a handoff for all the sessions. Active Cisco PDSN keeps the tunnel users counter as before; in standby Cisco PDSN, the number of counters increase.
 - Close all the sessions. The **show ip mobile tunnel** displays empty output for both active and standby Cisco PDSNs.
- With PMIP sessions:
 - Open 100 PMIP sessions , tunnel users counters match in both active and standby Cisco PDSNs, reflecting the number of users connected.
 - Perform a handoff for all the sessions. Active Cisco PDSN keeps the tunnel users counter as before; in standby Cisco PDSN, the number of counters increase.
 - Close all the sessions. The **show ip mobile tunnel** command displays empty output for an active Cisco PDSN; for standby Cisco PDSN, the output is not cleared. (Additional tunnel users are created during handoff.)

Workaround: None.

- CSCtb36803—Downstream AHDLC Fragmentation Not Working with ACCM As Zero in Cisco PDSN Release 5.0.

Downstream AHDLC fragmentation does not work with Asynchronous Control Character Map (ACCM) set to zero in Cisco PDSN Release 5.0. All asynchronous high-level data link control (AHDLC) packets are fragmented only in the outer IP, and not in the AHDLC. This fragmentation in the outer IP affects the IP packets sent to the mobile, where IP packets are greater than 1,460.

This issue is seen:

- for flows involving ACCM) set to zero.

Workaround: None.

Refer [Packet Fragmentation](#) section for more information.

Packet Fragmentation

The packet fragmentation is done using IP layer fragmentation and PPP layer fragmentation.

IP Layer Fragmentation

Cisco PDSN fragments IP packets at the IP layer, ensuring that the packet size is less than or equal to the interface MTU (default is 1,500 bytes). There is no GRE, PPP, or user IP header on the second fragment. So in IP layer fragmentation, if you capture packets using GRE.KEY as your filter, you will not capture the second fragment, because it does not have the GRE header in this packet fragment.

The below example snippet shows configuration of the IP layer fragmentation:

```
interface GigabitEthernet0/0
  mtu 1600
  no ip address
  no keepalive
!
interface GigabitEthernet0/0.11
  encapsulation dot1Q 11
  ip address 10.10.10.10 255.255.255.0
  ip mtu 1500
!
interface GigabitEthernet0/0.100
  encapsulation dot1Q 100
  ip address 20.20.20.20 255.255.255.224
!
interface GigabitEthernet0/0.200
  encapsulation dot1Q 200
  ip address 30.30.30.30 255.255.255.224
  ip mtu 1500
```

PPP Layer Fragmentation

In PPP fragmentation, the GRE header is included in both the packets. These are not IP fragments, as each packet has a different IP header. The GRE.KEY filter for a packet capture captures all PPP fragments related to the subscriber session based on GRE Key.

The below example snippet shows configuration of the PPP layer fragmentation:

```
interface Virtual-Template1
  ip unnumbered GigabitEthernet0/0.200
  peer default ip address pool sip-pool
  no keepalive
  ppp accm 0
  ppp authentication chap pap ms-chap optional
  ppp accounting none
  ppp ipcp dns 1.1.1.1 2.2.2.2
  ppp ipcp address unique
  ppp timeout idle 86400
```

Fragmentation in Cisco PDSN Release 4.0

In Cisco PDSN Release 4.0, the default packet fragmentation method is PPP fragmentation. You can use the CLI command **no cdma pdsn a10 ahdlc prefragment** to disable PPP fragmentation. If you use this command, Cisco PDSN fragments the packets at the IP layer.



Timesaver

Radio Access Network (RAN) PCFs can use PPP fragmentation for A10/GRE in the reverse direction, and the PCFs also accept IP layer fragmentation for A10/GRE forward direction. We recommend that you use the IP layer fragmentation because it increases PCF performance.

Fragmentation in Cisco PDSN Release 5.0

Cisco PDSN Release 5.0 uses IP layer fragmentation as the default setting. The PPP fragmentation support for Cisco PDSN will be provided in a later release.

If the PPP MTU on the virtual template is less than 1,500 bytes (default), no changes are required. You must set the MTU to less than 1,450 bytes to ensure that fragmentation is not required.

IP Layer Fragmentation with Default (1,500 Bytes) MTU:

To support IP layer fragmentation in Cisco PDSN Release 5.0, you must make the following changes when the default virtual interface does not specify an MTU. (In this case, the virtual interface will default to 1,500 bytes.)

- Cisco PDSN Release 5.0 offloads PPP byte-stuffing and cyclic redundancy check (CRC) generation to the IXP processor on the SAMI blade to increase performance.
- The MTU must be changed so that the power PC chip on the SAMI platform can send larger than 1,500 bytes to the IXP.
- The SAMI platform then allows the PPC to send the user's IP packet (1,500 bytes) along with the additional IP/GRE/PPP header (1,540 bytes), to the IXP.
- Set the MTU for GigabitEthernet 0/0 interface to 1,600 bytes. If you set the MTU to 1,600 bytes, the MTU of all sub-interface will also be set to 1,600 bytes. So if you have a sub-interface, such as a management interface that you do not want to set to 1,600 bytes, you must set the IP MTU for that sub-interface to 1,500.
- Ensure that the routes back to the PCFs use the sub-interface, which gets the MTU of 1,600 (that is, no "ip mtu xxxx" setting exists). In this case, the interface is GigabitEthernet 0/0.100.
- If the session redundancy between two SAMIs is enabled, ensure that the session redundancy is notified to the sub-interface, which has the MTU set for 1,500 bytes.

Resolved Caveats

The following caveats are resolved in Cisco IOS 12.4(22)XR:

• CSCsu70214

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>.

• CSCsw47076

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>.

• CSCsv48603

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>.

- CSCsx07114

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>.

- CSCsu50252

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>.

- CSCsy54122

A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>.

- CSCsy15227

Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

There are no workarounds that mitigate this vulnerability.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml>

- 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>.

- CSCsr18691

Cisco IOS devices that are configured with Cisco IOS Zone-Based Policy Firewall Session Initiation Protocol (SIP) inspection are vulnerable to denial of service (DoS) attacks when processing a specific SIP transit packet. Exploitation of the vulnerability could result in a reload of the affected device.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available within the workarounds section of the posted advisory.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ios-fw.shtml>

- CSCsu24505

Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available and are documented in the workarounds section of the posted advisory.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml>

- CSCsv75948

Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available and are documented in the workarounds section of the posted advisory.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml>

- CSCsx25880

A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml>.

- CSCsq24002

Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml>.

- CSCsx70889

Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.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>.

Product Documentation

Table 5 describes the product documentation that is available.

Table 5 *Product Documentation*

Document Title	Available Formats
<i>Release Notes for Cisco PDSN Release 5.0 in IOS Release 12.4(22)XR</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr/release/notes/124_22xrrn.html
<i>Command Reference for Cisco PDSN Release 5.0 in IOS Release 12.4(22)XR</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr/command/reference_xr/pdsn_5_0cr.html
<i>Cisco Packet Data Serving Node Release 5.0 for Cisco IOS Release 12.4(22)XR</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr/feature/guide/pdsn5_0_fcs.html

Related Documentation

Table 6 describes the related documentation that is available:

Table 6 *Related Documentation*

Document Title	Available Formats
<i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide, Release 12.4T</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/docs/ios/mwpdsn/configuration/guide/12_4t/mwp_12_4t_book.html
<i>Documentation on Cisco 7600 Series Router</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html
<i>Documentation on Cisco Catalyst 6500 Series Switch</i>	<ul style="list-style-type: none"> On Cisco.com at http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html
<i>Documentation on Caveats for Cisco IOS Release 12.4</i>	<ul style="list-style-type: none"> 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.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

© 2009 Cisco Systems, Inc.

All rights reserved.

