



Release Notes for Cisco GGSN Release 7.0 on the Cisco MWAM, Cisco IOS Software Release 12.4(9)XG

November 17, 2009

Cisco IOS Release 12.4(9)XG5

These release notes for the Cisco Gateway GPRS Support Node (GGSN) Release 7.0 on the Cisco Multi-processor WAN Application Module (MWAM) describe the enhancements provided in Cisco IOS Release 12.4(9)XG5. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4(9)XG, see the “[Cisco GGSN Caveats, Cisco IOS Release 12.4 XG](#)” section on page 15 and *Caveats for Cisco IOS Release 12.4 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.4* located on Cisco.com.

Technical Documentation Ideas Forum

Suggest ways Cisco technical documentation can be improved and better serve your needs. Participate in the Technical Documentation Ideas forum at: <http://www.cisco.com/go/techdocideas>

Contents

These release notes describe the following topics:

- [Introduction to Cisco GGSN on the Cisco MWAM, page 2](#)
- [System Requirements, page 3](#)
- [MIBs, page 7](#)
- [Limitations, Restrictions, and Important Notes, page 7](#)
- [New and Changed Information, page 10](#)



Americas Headquarters:

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

© 2009 Cisco Systems, Inc. All rights reserved.

- [Cisco GGSN Caveats, Cisco IOS Release 12.4 XG, page 15](#)
- [Cisco MWAM Caveats—Cisco IOS Release 12.4 XG, page 40](#)
- [Related Documentation, page 47](#)
- [Documentation Roadmap for Implementing GGSN Release 6.0 on the Cisco MWAM, page 49](#)
- [Obtaining Documentation and Submitting a Service Request, page 51](#)

Introduction to Cisco GGSN on the Cisco MWAM

The following sections describe Cisco GGSN and the Catalyst 6500 / Cisco 7600 Multi-processor WAN Application Module (MWAM).

- [Cisco GGSN Overview, page 2](#)
- [Cisco MWAM Overview, page 2](#)

Cisco GGSN Overview

Gateway GPRS support node (GGSN) is a service designed for Global System for Mobile Communications (GSM) networks. GSM is a digital cellular technology that is used worldwide, predominantly in Europe and Asia. GSM is the world's leading standard in digital wireless communications.

GPRS is standardized by the European Telecommunications Standards Institute (ETSI). The most common application of GPRS is expected to be Internet/intranet access. Cisco Systems' GPRS solution enables mobile wireless service providers to supply their mobile subscribers with packet-based data services in GSM networks.

GPRS introduces the following two new major network elements:

- Serving Gateway Support Node (SGSN)—Sends data to and receives data from mobile stations, and maintains information about the location of a mobile station (MS). The SGSN communicates between the MS and the GGSN. SGSN support is available from Cisco partners or other vendors.
- GPRS Gateway Support Node (GGSN)—A wireless gateway that allows mobile cell phone users to access the public data network (PDN) or specified private IP networks. The GGSN function is implemented on the Cisco Systems' router.

Combined 2.5G and 3G packet gateway support and interworking capability on the same node was introduced in Cisco GGSN Release 4.0.

Cisco MWAM Overview

With Cisco IOS Software Release 12.3(2)XB and later, Cisco GGSN software can run on the Cisco MWAM installed in a Catalyst 6500 series switch or Cisco 7600 series router.

The MWAM provides three processor complexes with dual processors used in two of the complexes and a single processor used in the remaining processor complex. This architecture provides five mobile wireless applications on one module.

The MWAM does not provide external ports but is connected to the switch fabric in the Catalyst 6500/Cisco 7600 chassis. An internal Gigabit Ethernet port provides an interface between each processor complex and the Supervisor module. Virtual Local Area Networks (VLANs) direct traffic from external ports via the Supervisor module to each mobile wireless application instance.

The MWAM provides an interface to the IOS image on the Supervisor module. The Supervisor module software enables a single session to be established to each application on the MWAM(s) in the chassis. Each session is used for configuring, monitoring, and troubleshooting application. For information on establishing sessions to mobile wireless application instances on the MWAM, refer to the [Cisco Multi-Processor WAN Application Module Installation and Configuration Notes](#):

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/mwam_icn.htm

**Note**

In this release, each application on the MWAM must be configured individually.

The software image that provides the mobile wireless application feature is downloaded through the Supervisor module and distributed to each processor complex on the MWAM(s). The same image is installed on all the processors in the MWAM.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(9)XG5 and includes the following sections:

- [Memory Recommendations, page 3](#)
- [Hardware and Software Requirements, page 4](#)
- [Determining the Software Version, page 5](#)
- [Upgrading to a New Software Release, page 5](#)

Memory Recommendations

Table 1 *Images and Memory Recommendations for Cisco IOS Release 12.4(9)XG5*

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco MWAM on the Cisco 7600	GGSN Standard Feature Set	c6svc5fmwam-g8is-mz.124-9.XG5.bin	128 MB	1 GB	RAM

Hardware and Software Requirements

Implementing Cisco GGSN Release 7.0 on the Cisco 7600 series Internet router platform requires the following hardware and software.

- Any module that has ports to connect to the network.
- Supervisor Engine 720, with a Multilayer Switch Feature Card, running Cisco IOS Release 12.2(18)SXE or later.

or

Cisco 7600 Series Supervisor Engine 32, with a Multilayer Switch Feature Card, running Cisco IOS Release 12.2(18)SXF or later.

For details on upgrading the Cisco IOS release running on the supervisor engine, refer to the “Upgrading to a New Software Release” section in the Release Notes.

- Cisco Multi-Processor WAN Application Module (MWAM) with the 1-GB memory option. The MWAM processors must be running Cisco IOS Release 12.4(9)XG or later.
- IPSec VPN Services Module (for security).



Note

Certain Cisco GGSN features, such as enhanced service-aware billing and GPRS tunneling protocol (GTP)-session redundancy, require additional hardware and software.

GTP-Session Redundancy

In addition to the required hardware and software above, implementing GTP-Session Redundancy (GTP-SR) requires at minimum:

- In a one-router implementation, two Cisco MWAMs in the Cisco 7600 series router, or
- In a two-router implementation, one Cisco MWAM in each of the Cisco 7600 series routers.

Enhanced Service-Aware Billing

In addition to the required hardware and software, implementing enhanced service-aware billing requires a Cisco Content Services Gateway (CSG) module in each Cisco 7600 series router. The CSGs must be running the same Cisco CSG software release, Release 3.1(3)C6(1) or later.

GTP Access Point Name-Aware Server Load Balancing

Support for GTP access point name (APN)-aware server load balancing (SLB) requires Cisco IOS Release 12.2(18) SRB and later on the supervisor engine module.



Note

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>

Determining the Software Version

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

```
Router# show version
Cisco IOS Software, MWAM Software (MWAM-G8IS-M), Version 12.4(9)XG5, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco
Systems, Inc.
```

Upgrading to a New Software Release

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

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

Upgrading IOS Image on MWAM

For information on upgrading IOS images on the MWAM, refer to the *Cisco Multi-Processor WAN Application Module Installation and Configuration Notes*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/mwam_icn.htm



Note

The image download process loads the IOS image onto the three processor complexes on the MWAM.

Upgrading ROMMON Software

To perform an ROMMON software upgrade, use the procedure provided in the *Cisco Multi-Processor WAN Application Module Installation and Configuration Notes*.

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. 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 U.S. 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 U.S. government regulations. When applicable, the 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.

The feature set tables have been removed from the Cisco IOS Release 12.4 release notes to improve the usability of the release notes documentation. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:


<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

<http://www.cisco.com/support/FeatureNav/FNFAQ.html>

Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.4 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

-
- Step 1** From the Cisco Feature Navigator home page, click **Feature**.
 - Step 2** To find a feature, use either “Search by full or partial feature name” or “Browse features in alphabetical order.” Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the text box on the left side of the web page.
 - Step 3** Select a feature from the left text box, and click the **Add** button to add a feature to the Selected Features text box on the right side of the web page.
- 

Note To learn more about a feature in the list, click the **Description** button below the left box.
-
- Repeat this step to add additional features. A maximum of 20 features can be chosen for a single search.
- Step 4** Click **Continue** when you are finished selecting features.
 - Step 5** From the Major Release drop-down menu, choose **12.4**.
 - Step 6** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 7** From the Platform Family drop-down menu, select the appropriate hardware platform. The “Your selections are supported by the following:” table will list all the software images (feature sets) that support the feature(s) that you selected.
-

Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.4, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

-
- Step 1** From the Cisco Feature Navigator home page, click **Compare/Release**.
 - Step 2** In the “Find the features in a specific Cisco IOS release, using one of the following methods:” box, choose **12.4** from the Cisco IOS Major Release drop-down menu.
 - Step 3** Click **Continue**.
 - Step 4** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 5** From the Platform Family drop-down menu, choose the appropriate hardware platform.
 - Step 6** From the Feature Set drop-down menu, choose the appropriate feature set. The “Your selections are supported by the following:” table will list all the features that are supported by the feature set (software image) that you selected.
-

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Limitations, Restrictions, and Important Notes

When using Cisco IOS Release 12.4(9)XG5, observe the following:

- Broadcast accounting is not supported with GTP Session Redundancy (GTP-SR) and wait accounting.
- The number of packet data protocol (PDP) contexts supported on a GGSN is dependent on the memory and platform in use and the GGSN configuration (for example, whether or not a method of Point-to-Point Protocol [PPP] has been configured to forward packets beyond the terminal equipment and mobile termination, whether Dynamic Feedback Protocol [DFP] is being used or the memory protection feature is enabled, and what rate of PDP context creation will be supported).



Note

DFP weighs PPP PDPs against IP PDPs with one PPP PDP equal to eight IP PDPs. One IPv6 PDP is equal to 8 IPv4 PDPs.

The Cisco MWAM can support up to 60,000 IPv4 PDP contexts per GGSN instance, with a maximum of 300,000 IPv4 PDP contexts per MWAM on which five GGSNs are configured, and up to 8,000 IPv6 PDP contexts per GGSN instance, with a maximum of 40,000 IPv6 PDP contexts per MWAM on which five GGSN are configured.

- Only five instances of the image can be loaded onto the MWAM.
- The same Cisco IOS image must be loaded onto all processor complexes on the MWAM.

- Session console is provided by TCP connection from the supervisor engine module (no direct console).
- Available bootflash memory for saving crash information files is 500 KB.
- Only five files can be stored in the bootflash filesystem.
- To avoid issues with high CPU usage, we recommend the following configurations:
 - To reduce the CPU usage during bootup, disable logging to the console terminal by configuring the **no logging console** command in global configuration mode.
 - To ensure that the Hot Standby Router Protocol (HSRP) interface does not declare itself active until it is ready to process the Hello packets from a peer, configure the delay period before the initialization of HSRP groups using the **standby delay minimum 100 reload 100 interface** configuration command on the HSRP interface.
 - To minimize issues with high CPU usage for additional reasons, such as periods of high PPP PDP processing (creating and deleting), disable the notification of interface data link status changes on all virtual template interfaces of the GGSN using the **no logging event link-status interface** command in interface configuration mode.

```

!
interface Virtual-Template1
description GGSN-VT
ip unnumbered Loopback0
encapsulation gtp
no logging event link-status
gprs access-point-list gprs
end

```

GTP Session Redundancy Limitations, Restrictions, and Important Notes

When configuring GTP-SR, note the following additional limitations and restrictions:

- The Active and Standby GGSNs have the same configuration, except for certain protocol-related configurations that need to be distinct such as the IP addresses of the HSRP-enabled interfaces and the remote IP addresses in the SCTP configuration.
- Each of the configurations must be completed in the same order on both of the units of the GTP-SR configuration.
- When loading or upgrading a new Cisco IOS GGSN image, both GGSNs must be loaded (virtually) together.
- On the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions are larger than the switchover timer. This enables requests sent during a switchover to be serviced by the newly Active GGSN rather than dropped.
- Remote Authentication Dial-In User Service (RADIUS) has been forced to use the IP address of a specified interface for all outgoing RADIUS packets using the **ip radius source-interface** global configuration command.
- PDP Contexts —Redundancy is not supported for the following types of PDP contexts. In the case of a switchover, these PDP contexts require re-establishment on the Standby GGSN once it becomes active.
 - PPP type PDP
 - PPP Regeneration / Layer 2 Tunneling Protocol (L2TP) access
 - Network Initiated

- **Timers**—Except for the session timer, GGSN timers are not synchronized to the Standby GGSN. When a switchover occurs, the timers on the newly Active GGSN are restarted with an increment to prevent many of them from expiring simultaneously.

When a PDP context is recreated on the Standby GGSN, the session timer is restarted with the elapsed time subtracted from the initial session timer value. Once the session expires on the Standby GGSN, the PDP context is deleted.

- **Counters**—If a switchover occurs, status counters, such as "cgprsAccPtSuccMsActivatedPdps," and some statistics counters will have a non-zero value that is the value of the counter at the time the switchover occurred. All other counters and statistics will be reset to zero.

If a GGSN reload occurs, all counters are set back to zero.

- **Sequence numbers** related to GTP signaling and data are not synchronized between the Active and Standby GGSNs.
- **Charging**—All pertinent information to establish charging on the Standby GGSN for a PDP context is synchronized, however, the user data related charging information for a PDP context is not. Therefore all CDRs in the previously Active GGSN that were not sent to the charging gateway are lost when a switchover occurs.
- Once a GTP-SR relationship is formed between two GGSNs, modifying the configuration of a GGSN might cause the GGSN to reload before the changes can be saved. To ensure that this does not occur, disable GTP-SR before modifying the configuration of a GGSN.

For information on disabling GTP-SR, see the “Configuring GTP Session Redundancy” chapter of the *Cisco GGSN Release 6.0 Configuration Guide*.

- In a GTP session redundancy (GTP-SR) environment, do not use the **clear gprs gtp pdp-context** command on the Standby GGSN. If you issue this command on the Standby GGSN, you are prompted to confirm before the command is processed. To confirm the state of a GGSN, issue the show gprs redundancy command.

Enhanced Service-Aware Billing Limitations, Restrictions, and Important Notes

When configuring a service-aware GGSN, note the following additional limitations and restrictions:

- RADIUS accounting must be enabled between the CSG and GGSN to populate the Known User Entries Table (KUT) entries with the PDP context user information.
- The CSG must be configured with the quota server (QS) addresses of all the GGSN instances.
- Service IDs on the CSG are configured as numeric strings that match the category IDs on the Diameter Credit Control Application (DCCA) server.
- If RADIUS is not being used, the Cisco CSG is configured as a RADIUS endpoint on the GGSN.
- On the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and CSG).

Specifically the SGSN $N3 \times T3$ must be greater than:

$2 \times \text{RADIUS timeout} + N \times \text{DCCA timeout} + \text{CSG timeout}$

where:

- 2 is for both authentication and accounting.
- N is for the number of diameter servers configured in the server group.

New and Changed Information

The following section lists new features and changed information in the Cisco IOS Release 12.4 XG releases:

- [New and Changed Information in Cisco IOS Release 12.4\(9\)XG5, page 10](#)
- [New and Changed Information in Cisco IOS Release 12.4\(9\)XG4, page 10](#)
- [New and Changed Information in Cisco IOS Release 12.4\(9\)XG3, page 10](#)
- [New and Changed Information in Cisco IOS Release 12.4\(9\)XG2, page 10](#)
- [New and Changed Information in Cisco IOS Release 12.4\(9\)XG1, page 13](#)
- [New and Changed Information in Cisco IOS Release 12.4\(9\)XG, page 13](#)

New and Changed Information in Cisco IOS Release 12.4(9)XG5

There are no new implementations or behavior changes in Cisco IOS Release 12.4(9)XG5.

New and Changed Information in Cisco IOS Release 12.4(9)XG4

There are no new implementations or behavior changes in Cisco IOS Release 12.4(9)XG4.

New and Changed Information in Cisco IOS Release 12.4(9)XG3

There are no new implementations or behavior changes in Cisco IOS Release 12.4(9)XG3.

New and Changed Information in Cisco IOS Release 12.4(9)XG2

Support for the following new feature is introduced in Cisco GGSN Release 7.0, Cisco IOS Release 12.4(9)XG2:

- **Fast PDP Delete**

To eliminate delays when deleting PDP contexts that occur because the SGSN is not responding to the delete PDP context requests, with Cisco IOS Release 12.4(9)XG2 and later, you can clear a PDP context without waiting for a response from the SGSN, or you can delete PDP contexts locally without sending a delete PDP context requests to the SGSN at all.

For detailed information about the Fast PDP Delete features, see the “Deleting Sessions” section in Chapter 3, “Configuring GTP Services on the GGSN” of the *Cisco GGSN Release 7.0 Configuration Guide*.

The following amendments and corrections will be made to the *Cisco GGSN Release 7.0 Configuration Guide*:

General Documentation Change

The documentation states that when a change from a Standby to an Active GGSN occurs, all counters are set back to zero. However, this statement is incorrect.

Please note that if a switchover occurs, status counters, such as "cgprsAccPtSuccMsActivatedPdps," and some statistics counters will have a non-zero value that is the value of the counter at the time the switchover occurred. All other counters will be reset to zero.

If a GGSN reload occurs, all counters are set back to zero.

Configuring Diameter/DCCA Interface Support

In the “Configuring Diameter/DCCA Interface Support” section of the “Configuring Enhanced Service-Aware Billing” chapter, the Abort Session Request / Abort Session Answer messaging description should include the following:

- Abort Session Request (ASR) / Abort Session Answer (ASA)—Note that no Failed-AVP is sent in an ASA when an incorrect ASR is sent from the DCCA server.

Configuring the DCCA Client Process on the GGSN

In the “Configuring the DCCA Client Process on the GGSN” section of the “Configuring Enhanced Service-Aware Billing” chapter, the description for the **ccfh** command is incorrect.

Currently, the **ccfh** command description is incorrectly documented as follows:

Command	Purpose
Router(config-dcca-profile)# ccfh {continue terminate retry_terminate}	<p>Configures the default Credit Control Failure Handling (CCFH) action to take on PDP contexts when a fault condition occurs.</p> <ul style="list-style-type: none"> • CONTINUE—Allows the PDP context and user traffic for the relevant category or categories to continue, regardless of the interruption. Quota management of other categories is not affected. • TERMINATE—Terminates the PDP context and the CC session. • RETRY—Allows the PDP context and user traffic for the relevant category or categories to continue. The DCCA client retries to send the CRR to an alternate server and if a failure-to-send condition occurs with the alternate server, the PDP context is terminated. <p>The default is terminate.</p> <p>A value from the DCCA server in a CCA overrides this default.</p>

The correct **ccfh** command description is the following:

Command	Purpose
Router(config-dcca-profile)# ccfh { continue terminate retry_terminate }	<p>Configures the default Credit Control Failure Handling (CCFH) action to take on PDP contexts when a fault condition occurs.</p> <ul style="list-style-type: none"> • continue—Allows the PDP context and user traffic for the relevant category or categories to continue, regardless of the interruption. Quota management of other categories is not affected. • terminate—Terminates the PDP context and the call control (CC) session. • retry_terminate—Allows the PDP context and user traffic for the relevant category or categories to continue. Hard-coded quota (1 GB) is passed to the CSG when the first DCCA server is unavailable. <p>The DCCA client retries to send the credit control request (CCR) to an alternate server and if a failure-to-send condition occurs with the alternate server, the PDP context is terminated.</p> <p>The default is terminate.</p> <p>A value from the DCCA server in a credit control answer (CCA) overrides this default.</p>

The following amendments and corrections will be made to the *Cisco GGSN Release 7.0 Command Reference*:

General Documentation Change

The documentation states that when a change from a Standby to an Active GGSN occurs, counters are set back to zero. However, this statement is incorrect. Please note that some counters, such as “cgprsAccPtSuccMsActivatedPdps,” are not set back to zero.

When a GGSN reload occurs, all counters are set back to zero.

The ccfh Command Description

The **retry_terminate** keyword option description in the **ccfh** command description is incorrect.

Currently, the **retry_terminate** keyword option is incorrectly documented as follows:

retry_terminate	Allows the PDP context and user traffic for the relevant category (or categories) to continue, regardless of the interruption while the DCCA client sends the CCR to an alternate Diameter server. If this attempt also fails, the session is terminated.
------------------------	---

The correct description for the **retry_terminate** keyword option is as follows:

retry_terminate	<p>Allows the PDP context and user traffic for the relevant category or categories to continue. Hard-coded quota (1 GB) is passed to the CSG when the first DCCA server is unavailable.</p> <p>The DCCA client retries to send the CCR to an alternate server and if a failure-to-send condition occurs with the alternate server, the PDP context is terminated.</p>
------------------------	---

New and Changed Information in Cisco IOS Release 12.4(9)XG1

There are no new implementations or behavior changes in Cisco IOS Release 12.4(9)XG1.

New and Changed Information in Cisco IOS Release 12.4(9)XG

Support for the following new features is introduced in Cisco GGSN Release 7.0, Cisco IOS Release 12.4(9)XG:

- **Authentication, Authorization, and Accounting Enhancements**

The maximum number of authentication, authorization, and accounting (AAA) method lists supported by the GGSN has been increased to 500. This enables up to 500 access-points to each have their own AAA method list.

- **Hold Back Timer**

The IP local pool holdback timer enables you to configure the GGSN to wait a specific amount of time before returning a newly-released IP address to the local pool when using a local IP address pool for allocating addresses to mobile stations.

The hold back timer ensures that an IP address recently released when a PDP session was deleted is not re-assigned to another PDP context before the IP-to-user relationship has been deleted from all back-end components of the system.

- **IPv6 PDPs**

Cisco GGSN supports IPv6 primary PDP context activation, and SGSN-initiated modification and deactivation procedures via IPv6 stateless autoconfiguration (as specified by RFC 2461 and RFC 2462). IPv6 over IPv4 tunnels configured on the Cisco 7600 supervisor engine module establish connectivity between isolated or remote IPv6 networks over an existing IPv4 infrastructure.

- **GTP APN-Aware SLB**

GTP APN-aware load balancing enables requests to be balanced across APNs. With GTP APN-aware load balancing, Cisco IOS SLB GTP maps that group APNs can be created and associated with a server farm under the virtual template. Multiple server farms can be defined in one virtual server, each supporting a different set of APNs.

- **PLMN and RAT Trigger Support for Service-Aware PDPs**

The Cisco GGSN supports public land mobile network ID (PLMN-ID) and radio access technology (RAT) triggers for service-aware PDPs.



Note With this release of the Cisco GGSN, all triggers must be explicitly enabled for both prepaid and postpaid users.

- **Command Line Interface Enhancements**

New commands have been introduced or existing commands have been modified, to support the following featurettes introduced in Cisco GGSN Release 7.0, Cisco IOS Release 12.4(9)XG.

- Clearing Global and Per-APN GPRS Statistics

The new **clear gprs statistics all** command clears all global and per-APN GPRS statistics cleared by the following commands:

- **clear gprs gtp statistics**
- **clear per-path statistics**
- **clear gprs access-point statistics all**
- **clear gprs service-aware statistics (includes CSG statistics)**
- **clear ggsn quota-server statistics**

- Displaying Per-SGSN Statistics

To assist in troubleshooting and diagnostics, the Cisco GGSN tracks various GTP global statistics on a per SGSN-path basis. These data path and control path counters can be displayed using the **show gprs gtp path statistics remote-address** privileged EXEC command.

Additionally, the GGSN can be configured to maintain a *history* for deleted paths. The data path and control path statistics for a deleted path can be displayed using the **show gprs gtp path statistics history** privileged EXEC command. To configure the maximum number of path entries for which you want the GGSN to maintain a history of the statistics, use the **gprs gtp path history** global configuration command.

For detailed information about the counters displayed using the **show gprs gtp path statistics history** command and the **show gprs gtp path statistics** command, refer to the command descriptions in the *Cisco GGSN Command Reference*.

- **MIB Enhancements for IPv6 PDP Support**

To support IPv6 PDPs, the **cgprsAccPtSecSrcViolNotif** trap, sent when a security violation has occurred, has been enhanced to send the notifications for IPv6 PDPs in addition to IPv4 PDPs.

The IPv6 support requires that the **ipv6 security verify source** access-point configuration command has been configured.

Cisco GGSN Caveats, Cisco IOS Release 12.4 XG

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

All caveats in Cisco IOS Release 12.4 and Cisco IOS Release 12.4 T are also in Cisco IOS Release 12.4(2)XG4.

For information on caveats in Cisco IOS Release 12.4, see *Caveats for Cisco IOS Release 12.4*.

http://www.cisco.com/en/US/products/ps6350/prod_release_notes_list.html

For information on caveats in Cisco IOS Release 12.4 T, see *Caveats for Cisco IOS Release 12.4T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.

http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html



Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats the most current list of caveats of any severity for any software release. To reach Bug Navigator II, Login to Cisco.com and click **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go directly to <http://www.cisco.com/support/bugtools>.

Table 1 summarizes the Cisco IOS Release 12.4 XG caveat activity:

Table 2 **Caveats Reference for Cisco IOS Release 12.4 XG**

DDTS Number	Open in Release	Resolved in Release
CSCec12299		12.4(9)XG2
CSCei14884		12.4(9)XG3
CSCek53232		12.4(9)XG1
CSCek53725	12.4(9)XG	12.4(9)XG2
CSCek54447	12.4(9)XG	
CSCek54782	12.4(9)XG	
CSCek60324	12.4(9)XG	
CSCek61309	12.4(9)XG	
CSCek67069	12.4(9)XG1	12.4(9)XG2
CSCek67598		12.4(9)XG2
CSCek68051	12.4(9)XG1	12.4(9)XG2 (closed)
CSCek68052	12.4(9)XG1 12.4(9)XG2	
CSCek73913		12.4(9)XG2
CSCek76015		12.4(9)XG2
CSCin99037		12.4(9)XG3
CSCir00949		12.4(9)XG2
CSCir01528		12.4(9)XG2

Table 2 Caveats Reference for Cisco IOS Release 12.4 XG (Continued)

DDTS Number	Open in Release	Resolved in Release
CSCir01561		12.4(9)XG2
CSCir01916		12.4(9)XG2
CSCir01949		12.4(9)XG2
CSCir02097		12.4(9)XG2
CSCir02107		12.4(9)XG2
CSCir02131		12.4(9)XG2
CSCir02173		12.4(9)XG2
CSCsd55969		12.4(9)XG2
CSCsd83175		12.4(9)XG2
CSCsd84784		12.4(9)XG2
CSCsd95616		12.4(9)XG2
CSCse07265		12.4(9)XG2
CSCse30648		12.4(9)XG2
CSCse49217	12.4(9)XG	
CSCse59614		12.4(9)XG2
CSCse07265		12.4(9)XG2
CSCse63424		12.4(9)XG2
CSCse83529		12.4(9)XG2
CSCsf13403		12.4(9)XG2
CSCsf18925		12.4(9)XG2
CSCsf20379		12.4(9)XG3
CSCsf25506	12.4(9)XG	
CSCsf96125		12.4(9)XG3
CSCsf97873		12.4(9)XG3
CSCsf99298		12.4(9)XG2
CSCsf99319	12.4(9)XG	
CSCsg03663	12.4(9)XG	
CSCsg05453		12.4(9)XG2
CSCsg18574	12.4(9)XG	12.4(9)XG2
CSCsg70355		12.4(9)XG1
CSCek73913		12.4(9)XG2
CSCsg73514		12.4(9)XG1
CSCsg76357	12.4(9)XG	
CSCsg76515	12.4(9)XG	
CSCsg83347		12.4(9)XG2

Table 2 **Caveats Reference for Cisco IOS Release 12.4 XG (Continued)**

DDTS Number	Open in Release	Resolved in Release
CSCsg83911		12.4(9)XG1
CSCsg85515		12.4(9)XG2
CSCsg91326		12.4(9)XG2
CSCsg92377		12.4(9)XG1
CSCsg92431		12.4(9)XG2
CSCsg94306		12.4(9)XG2
CSCsg94642		12.4(9)XG1
CSCsg96864	12.4(9)XG1 12.4(9)XG2	12.4(9)XG3
CSCsh06987		12.4(9)XG2
CSCsh02118		12.4(9)XG2
CSCsh12480		12.4(9)XG3
CSCsh17940		12.4(9)XG2
CSCsh18174		12.4(9)XG1
CSCsh18222		12.4(9)XG1
CSCsh20946		12.4(9)XG1
CSCsh21101		12.4(9)XG1
CSCsh24588		12.4(9)XG2
CSCsh34182	12.4(9)XG1	12.4(9)XG2
CSCsh59078		12.4(9)XG2
CSCsh60767		12.4(9)XG2
CSCsh69409		12.4(9)XG2
CSCsh82651		12.4(9)XG2
CSCsh87457		12.4(9)XG2
CSCsh88975		12.4(9)XG2
CSCsh90890		12.4(9)XG2
CSCsh17020		12.4(9)XG3
CSCsi22463		12.4(9)XG2
CSCsi40159		12.4(9)XG2
CSCsi44623		12.4(9)XG2
CSCsi89074		12.4(9)XG2
CSCsi92744		12.4(9)XG2
CSCsi99656		12.4(9)XG2
CSCsj15673		12.4(9)XG2
CSCsj16374		12.4(9)XG2
CSCsj34210	12.4(9)XG2	

Table 2 Caveats Reference for Cisco IOS Release 12.4 XG (Continued)

DDTS Number	Open in Release	Resolved in Release
CSCsj40040		12.4(9)XG2
CSCsj40311		12.4(9)XG2
CSCsj46809		12.4(9)XG2
CSCsj51090		12.4(9)XG2
CSCsj54102		12.4(9)XG2
CSCsj74145		12.4(9)XG2
CSCsj91542		12.4(9)XG2
CSCsk29283		12.4(9)XG3
CSCsk42759		12.4(9)XG3
CSCsk49429		12.4(9)XG3
CSCsk59944		12.4(9)XG3
CSCsl91117		12.4(9)XG3
CSCsk94202		12.4(9)XG3
CSCsl51652		12.4(9)XG3
CSCsl62609		12.4(9)XG3
CSCsm12214		12.4(9)XG3
CSCsm42890		12.4(9)XG3
CSCso84847		12.4(9)XG3
CSCsr22641		12.4(9)XG3
CSCsr41749		12.4(9)XG3
CSCsr41777		12.4(9)XG3
CSCsr78559		12.4(9)XG3
CSCsu89644		12.4(9)XG4
CSCsv06714		12.4(9)XG4
CSCsv11128		12.4(9)XG4
CSCsw78328		12.4(9)XG4
CSCsx19498		12.4(9)XG4
CSCsg22426		12.4(9)XG5
CSCsv30595		12.4(9)XG5
CSCsv34656		12.4(9)XG5
CSCsx25880		12.4(9)XG5
CSCsx35449		12.4(9)XG5
CSCsx70889		12.4(9)XG5
CSCsy15227		12.4(9)XG5
CSCtb77620		12.4(9)XG5
CSCtc07857		12.4(9)XG5

Caveats—Cisco IOS Release 12.4(9)XG5

This section contains the following types of caveats for the Cisco GGSN, Cisco IOS Release 12.4(9)XG5 maintenance release:

- [Open Caveats, page 19](#)
- [Resolved GGSN Caveats, page 19](#)
- [Resolved Miscellaneous Caveats, page 20](#)

Open Caveats

There are no known caveats open in Cisco IOS Release 12.4(9)XG5, Cisco GGSN Release 7.0.

Resolved GGSN Caveats

The following GGSN caveats are resolved in the Cisco IOS Release 12.4(9)XG5 image. This section describes only severity 1 and 2 caveats, and select severity 3 and 4 caveats.

- CSCsx35449

Description: The Cisco GGSN rejects Create PDP Context requests when more than 16Mb Guaranteed Bit Rate (GBR) is requested. This condition occurs only when the requested GBR is more than the supported bit rate for each PDP.

- CSCtb77620

Description: Due to missing 3GPP specifications, the Cisco GGSN might mix two PDP sessions into one when one of the following scenarios occurs:

- With an Update PDP Context request for a session with Tunnel Endpoint Identifier (TEID) 0x0000yyyy assigned in GTP version 1 (GTPv1) communication between the GGSN and SGSN, in the handover scenario in which GTPv1 exists between the source SGSN and GGSN and GTPv1 between the target SGSN and GGSN.
- With an Update PDP Context request for a session which was assigned in GTPv0 communication between the GGSN and SGSN with a flow label 0xyyyy, in the handover scenario in which a handover is made to GTPv1 between the target SGSN and GGSN while both source and target SGSNs talk with each other with GTPv1.

- CSCtc07857

Description: Under rare condition, a fatal error may occur with GTP parsing of PPP.

Resolved Miscellaneous Caveats

The following miscellaneous caveats are resolved in the Cisco IOS Release 12.4(9)XG5 image. This section describes only severity 1 and 2 caveats, and select severity 3 and 4 caveats.

- CSCsg22426

Description: A router running Cisco IOS may unexpectedly reload. The crashes can be very different in nature, but the crashinfo should show the IP Input process as the currently running process:

---- Partial decode of process block ----

Pid 84: Process "IP Input" stack 0x46C3C080 savedsp 0x46758540

This is seen when the router is configured for NAT and receives a fragmented skinny packet that it needs to reassemble and translate.

- CSCsv30595

Description: The Open Shortest Path First (OSPF) process might receive a fatal error when the router receives invalid OSPF messages.

- CSCsv34656

Description: A particular malformed OSPF message might cause the device to fail or operate unpredictably. This condition is seen when the OSPF receives a malformed OSPF message and the possible effects include the following:

- The router might receive a fatal error.
- Routing loops might form in the network.
- OSPF might control the CPU and drop adjacencies.
- The **show ip ospf database net** command output displays unwanted lines.

- CSCsx25880

Summary: 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>.

Note: The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 23, 2009, or earlier.

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

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

- 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>.

- CSCsy15227 Cisco IOS Software Authentication Proxy Vulnerability

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 web page.

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>

Caveats—Cisco IOS Release 12.4(9)XG4

This section contains the following types of caveats for the Cisco GGSN, Cisco IOS Release 12.4(9)XG4 maintenance release:

- [Open Caveats, page 21](#)
- [Resolved Caveats, page 21](#)

Open Caveats

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XG4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no caveats are open in Cisco IOS Release 12.4(9)XG4, Cisco GGSN Release 7.0.

Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.4(9)XG4. This section describes only severity 1 and 2 caveats, and select severity 3 and 4 caveats.

- CSCsq31776

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>.

- CSCsu89644

Description: The Cisco GGSN appears to not respond to node alive requests sent by the secondary charging gateways using a TCP path. Additionally, if the node alive request is sent over UDP from the active charging gateway, the GGSN sends the response over TCP, if the TCP link is up.

These conditions exist for charging gateways using a TCP path.

- 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>.

- CSCsv06714

Description: When a Cisco GGSN receives a Credit Control Answer (CCA) with a 5012 result code for a service, it does not correctly process the CCA, and keeps “service in waiting” for the CCA state, and does not send any response to the CSG.

- CSCsv11128

Description: If the user location information element (IE) is not received in a Create PDP Context request, the Cisco GGSN does not include USER-LOCATION-INFO AVP when requesting quota for a prepaid service.

This condition is seen when the user location information IE is not received in a Create PDP Context request even though the Routing Area Identity (RAI) is sent in the Create PDP Context request.

- CSCsw78328

Description: Issuing the **clear gprs statistics** command when there are active PDP contexts might cause subsequent SNMP GETS for the cgprsAccPtActivePdps OID to report a value that is too high.

For example, if there are 100 active PDP contexts when the **clear gprs statistics** command is issued, and later these 100 active PDP contexts are disconnected, and even later, 50 new PDP contexts connect, the cgprsAccPtActivePdps will show 150 active PDP contexts while the show command will display the correct value of 50. Counters clear after a reload.

- CSCsx19498

Description: The Cisco GGSN does not encode the International Mobile station Equipment Identity Software Version (IMEISV) value in the format required by the 3GPP Release 7 specification.

This condition is seen when a GTP message from the SGSN includes the IMEISV value.

Caveats—Cisco IOS Release 12.4(9)XG3

This section contains the following types of caveats for the Cisco GGSN, Cisco IOS Release 12.4(9)XG3 maintenance release:

- [Open Caveats, page 23](#)
- [Resolved Caveats, page 23](#)

Open Caveats

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XG3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no caveats are open in Cisco IOS Release 12.4(9)XG3, Cisco GGSN Release 7.0.

Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.4(9)XG3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCei14884

Description: During a GGSN switchover, a Cisco RF-MIB trap is sent to the management station that indicates that the GGSN instance 1 changed its state: unit state is displayed as “negotiation,” and the peer unit state is “disabled” when it should be “active.” Also the “.1.3.6.1.4.1.9.9.176.2.0.1: Switch of activity occurred (cRFStatusUnitId=0, sysUpTime=31-8,” should not be expected when the switchover occurs.

- CSCin99037

Description: When a PDP context is created with a remote port other than the default port (2123/2152), the Cisco GGSN will not display path statistics. Also, the **show gprs gtp path all** command displays the wrong remote ports.

- CSCsf20379

Description: The Cisco GGSN might not send the quotaPushFail trap when GGSN quota server debugging, enabled using the **debug ggsn quota-server** command, is disabled.

- CSCsf96125

Description: The Cisco GGSN does not decrement the time-to-live (TTL) value before sending the packet towards the Gigabit interface.

This condition occurs when the IP packet is fragmented. If the IP packet is not fragmented, the GGSN decrements the TTL by 1 to 127 before sending it out to the Gigabit interface.

- CSCsf97873

Description: On an access point (APN) enabled for PPP regeneration, creating an L2TP from the GGSN to the L2TP network server (LNS) shows inconsistent behavior in time-to-live (TTL) handling between the uplink and downlink.

Configuration: MS Client—SGSN—(GTP)—GGSN—(L2TP)—LNS

Scenario 1: The MS client sends an Internet Control Message Protocol (ICMP) packet with 1432 bytes of ICMP data. No IP fragmentation occurs.

Scenario 2: The MS client sends an ICMP packet with 1433 bytes of ICMP data. IP fragmentation occurs.

When packets from Scenario 2 enter the GTP tunnel or the L2TP tunnel, the total size is 1501 bytes and the packet must be fragmented by tunnel endpoints (the SGSN, GGSN, and LNS).

Protocol header calculation:

- GTP: IP (20) + UDP (8) + GTP (12) + IP (20) + ICMP Header (8) = 68 byte
- L2TP: IP (20) + UDP (8) + L2TP (8) + PPP (4) + IP (20) + ICMP Header (8) = 68 bytes.

In the uplink direction, from the SGSN, to the GGSN, to the LNS, the TTL value of the packet is always 128 for Scenarios 1 and 2. So the TTL is not decreased at the GGSN. In the downlink direction, from the LNS, to the GGSN, to the SGSN, the behavior is different. In the case of Scenario 1, the TTL value is decreased by 1 by the GGSN. In the case of Scenario 2, the TTL is not changed by the GGSN. The TTL value stays the same.

- CSCsg96864

Description: A Cisco router running the Cisco GGSN Release 7.0 software exhibits the following incorrect behavior when a protocol error is received in a CCA.

- When CCFH=terminate, and the protocol error is received in a CCA(Initial) and the subsequent CCA(Final), the PDP context is not deleted.
- Upon receipt of protocol errors 3002 and 3005, the GGSN does not failover to a second server.
- When CCFH=continue, and the protocol error is received in a CCA(Initial), the PDP context is converted to postpaid, but the create PDP context response is not sent.

- CSCsh12480

Cisco IOS software configured for Cisco IOS firewall Application Inspection Control (AIC) with a HTTP configured application-specific policy are vulnerable to a Denial of Service when processing a specific malformed HTTP transit packet. Successful exploitation of the vulnerability may result in a reload of the affected device.

Cisco has released free software updates that address this vulnerability.

A mitigation for this vulnerability is available. See the “Workarounds” section of the advisory for details.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-iosfw.shtml>.

- CSCsi17020

A series of segmented Skinny Call Control Protocol (SCCP) messages may cause a Cisco IOS device that is configured with the Network Address Translation (NAT) SCCP Fragmentation Support feature to reload.

Cisco has released free software updates that address this vulnerability. A workaround that mitigates this vulnerability is available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sccp.shtml>.

- CSCsk29283

Description: On a Cisco MWAM running the Cisco GGSN software, if an SGSN does not include a recovery IE in its initial signaling requests, and then it includes the recovery IE in subsequent requests, the GGSN will initiate a path cleanup (deleting all existing PDPs on the path) because the path recovery changed.

This condition exists only when the SGSN does not include the recovery IE in the initial requests and includes it in subsequent requests.

- CSCsk42759

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsk49429

Description: On a Cisco router running the Cisco GGSN software, the router might reload during the rare situations when a heavy traffic load is occur along with the following conditions:

- The SGSN sends a different recovery IE in an update PDP context request
- Echo request are enabled on the GGSN and the GGSN is running at high CPU with a lot of PDP context deletions occurring.

- CSCsk59944

Description: The Cisco GGSN charging release configuration can be modified using the **gprs charging release** global configuration command while there are charging records pending in the system.

- CSCsl91117

Description: The Cisco GGSN allows charging destination port to be changed using the **gprs charging port** command when there are CDRs in the pending queue or in a closed state.

- CSCsk94202

Description: When there is data being processed through PDP contexts, and the contexts are deleted at the same time, the GGSN reloads. This condition occurs when the timing is within the few milliseconds the PDP is being deleted.

- CSCsl51652

Description: The PDP create and last access time displayed in the output of the **show gprs gtp pdp-context tid** command becomes incorrect after two GGSN failovers.

- CSCsl62609

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-sip.shtml>.

- CSCsm12214

Description: The Cisco GGSN does not send pending CDRs from the pending queue to the charging gateway. This condition is seen when the TCP connection has terminated due to no response from charging gateway for the DTR and not even after subsequent node alive.

- CSCsm42890

Description: On a Cisco MWAM processor running the Cisco GGSN application, there is a possibility of an input queue wedge on the GTP virtual access interface preventing data traffic for the affected APNs. This condition occurs only if the access point (APN) is configured with the redirect-all feature and the mobile station sends upstream packets with the TTL option in the IP header set to 1.

- CSCso84847

Description: If a mobile subscriber includes 3 B containing 0x0 at the end of the QoS IE, the GGSN logs the following message, and fails to establish a tunnel:

```
%GTP-0-GTPv1PACKETPARSINGERROR : GSN: GSN: [IP_address], TEID: [hex], APN: [chars],
Reason:The mandatory IE is incorrect
```

- CSCsr22641

Description: If a Service-Auth request is received for a service in IDLE state while the PDPs are being deleted, the service-aware PDP contexts become stuck on the GGSN and cannot be deleted. This condition occurs only if the Service-Auth request is received for a service in IDLE state when a PDP is in the process of being deleted.

- CSCsr41749

Description: On a Cisco router running the Diameter application, parsing of a capabilities exchange answer (CEA) fails if the Diameter server includes the origin-state-id attribute with the mandatory bit set.

This condition occurs only if the server includes the origin-state-id attribute with the mandatory bit set.

- CSCsr41777

Description: On a Cisco router running the Diameter credit control application (DCCA), parsing of capabilities exchange answer (CEA) fails if the Diameter server includes the origin-state-id attribute with the mandatory bit set. Additionally, if the GGSN does not send the origin-state-id attribute in the credit control response (CCR) and the attribute is received in credit control answer (CCA), it is ignored.

These conditions occur only if the Diameter server includes the origin-state-id attribute with the mandatory bit.

- CSCsr78559

Description: When reporting usage owing to the Quota Holding Timer (QHT) expiry, the Cisco GGSN includes the Requested-Service-Unit AVP in the Multiple Services Credit Control (MSCC).

This condition is seen when the GGSN is sending a CCR-Update owing to the QHT expiration.

Caveats—Cisco IOS Release 12.4(9)XG2

This section contains the following types of caveats for the Cisco GGSN, Cisco IOS Release 12.4(9)XG2 maintenance release:

- [Open Caveats, page 27](#)
- [Resolved Caveats, page 28](#)
- [Closed Caveat, page 35](#)

Open Caveats

This section documents possible unexpected behavior by Cisco IOS Release 12.4(9)XG2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

The following caveats are open in the Cisco IOS Release 12.4(9)XG2, Cisco GGSN Release 7.0.

- CSCek68052

Description: At bandwidths below 50 Mbps, packet drops are seen for IPV6 PDP contexts on GGSN.

With 8,000 PDP contexts across 500 VRF APNs with 16 IPv6 PDP's per VRF APN, these drops are seen as follows:

1. With 128-byte packet size, the drops occur at 7.2 Mbps.
2. With 256-byte packet size, drops occur at 11.1 Mbps.
3. With 512-byte packet size, drops are seen at 22.94 Mbps.
4. With 1400-byte packet size, drops are seen at 47.02 Mbps.

Workaround: There is currently no known workaround.

- CSCsg96864

Description: A Cisco router running the Cisco GGSN Release 7.0 software exhibits the following incorrect behavior when a protocol error is received in a CCA.

- a. When CCFH=terminate, and the protocol error is received in a CCA(Initial) and the subsequent CCA(Final), the PDP context is not deleted.
- b. Upon receipt of protocol errors 3002 and 3005, the GGSN does not failover to a second server.
- c. When CCFH=continue, and the protocol error is received in a CCA(Initial), the PDP context is converted to postpaid, but the create PDP context response is not sent.

Workaround: There is currently no known workaround.

- CSCsj34210

Description: When a CDR transfer fails, the charging gateway is not changed to an UNDEFINED state. This condition occurs when the path protocol is TCP and the charging gateway is brought down by shutting the interface.

Workaround: There is currently no known workaround.

Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.4(9)XG2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec12299

Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

Workarounds are available to help mitigate this vulnerability.

This issue is triggered by a logic error when processing extended communities on the PE device.

This issue cannot be deterministically exploited by an attacker.

Cisco has released free software updates 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-20080924-vpn.shtml>.

- CSCek53725

Description: During the opening of 8000 PPP regenerated PDPs at 20 cps, the CPU reaches more than 90% after 5000 PDPs are opened.

- CSCek67069

Description: A Cisco GGSN passes IPv4 data of less than 100 Mbps. This condition occurs for packets less than 512 bytes when there are 500 VRFs.

- CSCek67598

Description: The “rcvd ipv6 signal msg” counter displayed in the **show gprs gtp statistics** command output is incremented twice when a duplicate GTPv1 IPv6 create PDP context request is received.

- CSCek73913

Description: The GGSN takes a long time to delete thousands of PDPs when the PDPs are cleared using the **clear gprs gtp pdp-context** command. This condition occurs when the SGSN does not respond to the delete PDP context requests sent by the GGSN.

For more information about the fix for this defect, see the “Configuring GTP Services on the GGSN” chapter of the *Cisco GGSN Release 7.0 Configuration Guide*.

- CSCek76015

Description: Fast deleting service-aware PDPs stops after the internal delete credit is reached (default 1000 PDPs).

This condition occurs with only service-aware PDPs when the **no-wait-sgsn** or the **local-delete** keyword options have been specified with the **clear gprs gtp pdp-context access-point** command and the SGSN is responding (not a condition for using the Fast PDP Delete feature).

- CSCir00949

Description: The counters that are displayed in the **show gprs gtp path statistics remote-address** command output that are related to roaming PDPs are not incremented. With this fix, three new counters, Roaming trusted PDPs, Roaming non-trusted PDPs, and Non-roaming PDPs replace the previous roaming PDP counter.

- CSCir01528

Description: When a Cisco GGSN is configured to allocate IP addresses for an APN from a RADIUS server, if the RADIUS server does not return an IP address for a particular user, there might be an incorrect syslog message displayed that indicates that no RADIUS server is available.

- CSCir01561

Description: When a GTP update request is received from an SGSN without a change of SGSN address or change of QoS, and with only any of the following attributes changes, ms-timezone, RAT, and User Location Info, the accounting interim record sent to the AAA server as part of the update request procedure does not include new values for these attributes.

- CSCir01916

Description: The “cef_up_byte” count in the **show gprs gtp pdp tid** command output for a PPP PDP which is terminating at the GGSN shows 4 bytes less. The upstream data count in the CDR also shows 4 bytes less. This condition is experienced only for a PPP PDP in a CEF path.

- CSCir01949

Description: The common counters for the uplink and downlink traffic PDUs are not incremented in the **show gprs access-point statistics** command output for IPv6 traffic.

- CSCir02097

Description: When redundant GGSNs and system accounting are configured, and the Active GGSN is reloaded using the **reload** command, the Active GGSN sends an Accounting-Off message to the AAA server. This condition occurs only when a redundant configuration exists, system accounting is enabled, and the **reload** command is issued on the Active GGSN.

- CSCir02107

Description: When a path is created without the recover information element (IE) being received from the SGSN, and the path is updated later with a valid recovery IE, the standby GGSN does not update the recover IE with the new value.

This condition occurs only if the SGSN is incapable of sending a recovery IE in the create PDP context request.

- CSCir02131

Description: When a PPP PDP (terminated on GGSN) is created with duplicate mobile IP address, the request is not rejected. This condition occurs only for PPP PDPs.

- CSCir02173

Description: On a Cisco router running the Cisco GGSN software, source and destination address validation of TPDU is not occurring in the case of PPP-PDP terminating on the GGSN and PPP-regenerated PDPs when security verify source, destination, or access list is configured under APN. This validation is also not occurring when traffic is initiated from a network behind mobile station. This condition is observed when **ip cef** is configured.

- CSCsd55969

Description: The GGSN allows the DCCA feature and the OCS server selection feature to be configured simultaneously. These features do not work together and the GGSN should print an error message to the screen when either one of the features is already configured and an attempt is made to configure the other.

- CSCsd83175

Description: The Cisco GGSN Redirect All feature (enabled using the **ipv6 redirect all** access point configuration command) and the Redirect Inter-Mobile feature (enabled using the **ipv6 redirect intermobile** access point configuration command) do not work as expected for IPv6 PDP contexts.

- CSCsd84784

Description: The **no ipv6 ipv6-address-pool** command does not negate the **ipv6 ipv6-address-pool** command configuration. Therefore, the dynamic address allocation method cannot be restored to the default value. This condition occurs when the **no ipv6 ipv6-address-pool** command is used.

- CSCsd95616

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates 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-20080924-multicast.shtml>.

- CSCse07265

Description: When defining an IP SLA probe with a reaction event of TIMEOUT or CONNECTION LOSS and setting the probe to generate a trap, a syslog message is not generated when it should be.

- CSCse30648

Description: When the **gprs radius attribute quota-server ocs-address** global configuration command is configured and a prepaid PDP context is created with an external quota server interfacing with the Cisco CSG in a enhanced service-aware billing configuration, the service-aware details of the PDP context displays the DCCA profile name even though the DCCA is not used for this user.

- CSCse59614

Description: The **ipv6 ipv6-access-group** command's **uplink** and **downlink** keyword options are not registered correctly in the running configuration. Instead, the keywords "up" and "down" are used.

- CSCse63424

Description: The "redirect-all" counter displayed in the **show gprs gtp pdp tid** command output might not increment for IPv6 PDPs.

This condition occurs when IPv6 redirect is enabled on an APN.

- CSCse83529

Description: When a PDP context is created for a pre-paid APN, the encoding of quota push is incorrect and the PDP is held in a PENDING_QP category state. Therefore, there is no GTP response returned to the SGSN.

- CSCsf13403

Description: Spurious memory access might be seen when configuring the **encapsulation gtp** command under the virtual template. Additionally, the **gprs access-point-list** command might not take effect.

This condition occurs when configuring GTP under the virtual template.

- CSCsf18925
Description: The GGSN might reload while performing multiple SNMP operations.
- CSCsf99298
Description: When a Neighbor Advertisement is sent by the GGSN in response to a unicast Neighbor Solicitation, the “S” bit in the response is not set.
This condition occurs when a Neighbor Solicitation is sent by an IPv6 PDP to the SGSN.
- CSCsg05453
Description: The **show gprs gtp pdp tid** command display is incorrect for a PDP with a Release 98 QoS profile.
- CSCsg18574
Description: When certain GGSN security features are enabled, GTP byte and packet counters are not updated correctly. Also, ICMP redirects are not sent in some cases.
- CSCsg83347
Description: The MIB objects `cgprsAccPtName` and `cgprsAccPtMsIsdnSuppressedValue` might not accept a null string.
- CSCsg85515
Description: When a Standby GGSN becomes active, and there is a pending PDP request, the GGSN doesn’t clear the counter after it becomes active.
- CSCsg91326
Description: When the Diameter server experiences delayed responses and the Cisco GGSN keeps generating new authorization requests, the Gi0/0 interface on the Cisco MWAM shows the input queue size increase all the way to the maximum value. This causes the GGSN to encounter a path failure to the SGSN and the active PDP contexts are deleted. This condition occurs only when responses from the Diameter server are delayed.
- CSCsg92431
Description: The total data dropped counter does not increment for IPv6 PDPs. This condition occurs when a TPDU is dropped at the GGSN for an IPv6 PDP.
- CSCsg94306
Description: The ACL matches counter does not increment for IPv6 PDPs. This condition occurs when an IPv6 ACL is added to an IPv6 APN in the downlink direction.
- CSCsh02118
Description: The “ms init ipv6 pdp activation” counter displayed for access point statistics does not increment for GTPv0 IPv6 PDPs. This condition occurs only with GTPv0 IPv6 PDPs.
- CSCsh06987
Description: The “unexpected_data_msg” counter increments incorrectly in the **show gprs gtp statistics** command output.
This condition occurs when data messages are dropped at the GGSN.
- CSCsh17940
Description: When multiple PDPs with different IMSI s and the same MSIDNs are created on an APN using DHCP addressing, the second create PDP context request deletes the PDP on the Standby GGSN, but the PDP remains on the Active GGSN.

- CSCsh24588

Description: The GGSN might not respond to an IPv6 router solicitation from the MS when IPv6 redirect is enabled. This condition occurs only when an IPv6 PDP is created on an APN which has the IPv6 redirect-all feature enabled.

- CSCsh34182

Description: A Cisco GGSN responds to out-of-order GTP packets from the CSG for non-existent PDP contexts with a cause code of 201. This condition does not affect the correct functioning of the system, and occurs only when the CSG is experiencing periods of overload.

- CSCsh59078

Description: SNMP small chunk leaks while setting the ACC-PT-MIB objects. This condition occurs when a “set” is performed for any of the objects belong to the cgprsAccPtTable and all the tables augmented to cgprsAccPtTable.

The chunk leaks can be observed by issuing the show memory deb leaks chunk command after a “set.”

- CSCsh60767

Description: When an APN is configured to generate a probe using the **ip probe path** command, when a PDP context is established, the following might occur:

1. If the APN is configure for RADIUS accounting, the probe will be sent before the accounting-start message. The accounting-start message contains the framed-IP address necessary to populate the B sticky table.

A downstream RLB does not have the framed-IP address when the probe arrives and will either drop (ip slb route framed-ip deny) the probe packet or forward it to the routing table. The FWLB behind the load-balanced real is respectively not populated, or incorrectly populated 50% (if there are two reals) of the time because the routing table will point to one load-balanced real address. If server-initiated traffic is generated before preceding client originated traffic, traffic will go to the wrong real 50% of the time.

2. If the APN is also configured for wait-accounting, the probe is sent regardless of the success of the accounting flow. Also, as a result of RADIUS accounting failure, no PDP context is established.

Regardless of IP address allocation (local pool or RADIUS server), the framed-IP address is available either in the access-accept message or the accounting-start message, and not in the access-request message. Therefore, there is no dynamic workaround.

- CSCsh69409

Description: The “signalling_msg_dropped” counter in the **gprs gtp statistics** command output is not incremented and the GGSN does not process the packet further if the comprehension bit is not set.

This condition occurs when the GGSN processes messages with an unsupported extension header.

- CSCsh82651

Description: On a Cisco router running the Cisco GGSN software, path history (**show gprs gtp path history** command) is not being deleted when a lower value is set using the **gprs gtp path history** global configuration command. This issue is seen when GPRS service is disabled and enabled again.

- CSCsh87457

Description: The APN name might display with some junk characters in the running configuration when the object `cgprsAccPtName` is set to null through SNMP.

This condition occurs after setting `cgprsAccPtName` to null through SNMP.

- CSCsh88975

Description: Traffic for PPP regenerated PDP fails with CEF.

- CSCsh90890

Description: Incorrect response from the GGSN occurs for any traffic sent over TCP for the charging gateway.

- CSCsh97579

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>.

- CSCsi22463

Description: %ALIGN-1-FATAL:Illegal access to a low address on signalling stress test

System crash and tracebacks occur during a signalling stress test (60,000 PDPs, send updates, perform handoffs, delete PDPs, and repeat). After several hours of this activity, the crash and tracebacks occurred.

- CSCsi40159

Description: The behavior of the `gprs slb vserver ip next-hop ip ip` command and the corresponding MIB object `cGgsnSlbVserNextHopAddress` might be inconsistent.

- CSCsi44623

Description: Setting `cgprsCgPartialCdrGenEnableAll` to true or false might not work as expected in certain scenarios.

- CSCsi89074

Description: Tracebacks are seen (via the `show alignment` command) in the GGSN when GTPv0 PPP PDPs are created, and then, if the `no service alignment detection` command is configured, the GGSN crashes.

- CSCsi92744

Description: Static PDPs are created without user-requested IPCP values.

- CSCsi99656

Description: When a redirect request is sent from the primary charging gateway (CG) with a secondary CG as the address of the recommended node, the Cisco GGSN does not send the redirect response to the primary CG. The CG which sends the redirect request expects a redirection response from the GGSN, however the GGSN sends the redirection response to the recommended node. Therefore, there is a sequence number mismatch on the GTP header and the CG that sent the request goes into “waiting for a redirect response” state.

- CSCsj15673

Description: The Cisco GGSN reports spurious memory access when the TCP socket use for charging functions is being cleared. This condition occurs only for the TCP charging path and when there are pending CDRs.

- CSCsj16374
Description: On a Cisco router running the Cisco GGSN software, MS-requested primary and secondary DNS values are not honored. This condition is seen when the create PDP context request is for an IPv6 static PDP.
- CSCsj40040
Description: On a Cisco MWAM running the Cisco GGSN software, if an ACL is configured under the APN for inspection of mobile traffic, and if this ACL includes the ttl option, the ACL will not be applied. This condition occurs only if the ACL is defined for inspection of ttl in the mobile IP packets.
- CSC40311
Description: On a Cisco router running the Cisco GGSN software, when a create PDP context is received with an extension header to the GTP header, and the extension header has a length of 0 bytes, the GGSN might reload. The conditions that lead to this reload rarely occur.
- CSCsj46809
Description: When a Redirection Request message is sent from the primary charging gateway, the GGSN does not send the Redirection Response message to the primary gateway and the “Redirect Resp Rcvd” field is not incremented.
- CSCsj51090
Description: On a Cisco router running the Cisco GGSN software in redundant mode, after a switchover occurs, the newly active GGSN cannot forward traffic on PDP contexts that belong to some access point. This condition occurs only on a few APNs after a switchover from a current active to the standby GGSN occurs.
- CSCsj54102
Description: The Fast Delete feature command options are not available when the GGSN is in global maintenance mode and the APNs are not in maintenance mode.
 This condition occurs when the APNs are not in maintenance mode.
- CSCsj74145
Description: On a Cisco MWAM running the Cisco GGSN software, if an Error-Indication is received from an SGSN on a GTPv1 path, which leads to PDP context deletion on the GGSN, the corresponding Accounting-Stop will have the Acct-Terminate-Cause as “Unknown,” instead of “Nas-Error.” This condition occurs only when an error-indication is received on a GTPv1 path. If the SGSN path is a GTPv0, the Acct-Terminate-Cause is “Nas-Error.”
- CSCsj91542
Description: The CDRs sent to the charging gateway accumulate volume counter values including values sent in prior CDRs. This condition occurs when the charging profile configured in the GGSN does not have SGSN change limit and when the configured send buffer limit is reached as a result of a sequence of SGSN change messages. The CDR is closed and sent but without resetting the counters.

Closed Caveat

The following caveat is closed in Cisco IOS Release 12.4(9)XG2.

- CSCek68051

Description: Throughput measurement for all IPv4 packet sizes differs base on two types of flows. This difference occurs when traffic is sent across 60,000 PDPs on the Cisco GGSN, created across 500 VRF APNs with 120 PDPs per VRF APN, at 80%:20% downstream:upstream.

- Flow 1—Traffic is sent at the rate of 84 Mbps with 67 Mbps downstream and 16.9 Mbps upstream with the first packet sent on the first PDP on VRF-APN1, the second packet sent to the first PDP on VRF-APN2, and so on, up to VRF-APN500. During this flow, the CPU on the GGSN is in the 82% to 89% range.
- Flow 2—Traffic is sent is at rate of 108.36 Mbps with 86.6 Mbps downstream and 21.6 Mbps upstream with the first packet sent on the first PDP on VRF-APN1, the second packet sent to the second PDP on VRF-APN1, and so on, up to 120 PDPs in VRF-APN1, and then repeating the same for VRF-APN2, and so on, up to VRF-APN500. During this flow, the CPU on the GGSN is in the 75% to 84% range.

Caveats—Cisco IOS Release 12.4(9)XG1

This section contains the following types of caveats for the Cisco GGSN, Cisco IOS Release 12.4(9)XG1 maintenance release:

- [Open Caveats, page 35](#)
- [Resolved Caveats, page 36](#)

Open Caveats

This section documents possible unexpected behavior by Cisco IOS Release 12.4(9)XG1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

The following caveats are open in Cisco IOS Release 12.4(9)XG1, Cisco GGSN Release 7.0.

- CSCek67069

Description: A Cisco GGSN passes IPv4 data of less than 100 Mbps. This condition occurs for packets less than 512 bytes when there are 500 VRFs.

Workaround: Implement fewer VRFs.

- CSCek68051

Description: Throughput measurement for all IPv4 packet sizes differs base on two types of flows. This difference occurs when traffic is sent across 60,000 PDPs on the Cisco GGSN, created across 500 VRF APNs with 120 PDPs per VRF APN, at 80%:20% downstream:upstream.

- Flow 1—Traffic is sent at the rate of 84 Mbps with 67 Mbps downstream and 16.9 Mbps upstream with the first packet sent on the first PDP on VRF-APN1, the second packet sent to the first PDP on VRF-APN2, and so on, up to VRF-APN500. During this flow, the CPU on the GGSN is in the 82% to 89% range.

- Flow 2—Traffic is sent at rate of 108.36 Mbps with 86.6 Mbps downstream and 21.6 Mbps upstream with the first packet sent on the first PDP on VRF-APN1, the second packet sent to the second PDP on VRF-APN1, and so on, up to 120 PDPs in VRF-APN1, and then repeating the same for VRF-APN2, and so on, up to VRF-APN500. During this flow, the CPU on the GGSN is in the 75% to 84% range.

Workaround: There is currently no known workaround.

- CSCek68052

Description: At bandwidths below 50 Mbps, packet drops are seen for IPV6 PDP contexts on GGSN.

With 8,000 PDP contexts across 500 VRF APNs with 16 IPv6 PDP's per VRF APN, these drops are seen as follows:

1. With 128-byte packet size, the drops occur at 7.2 Mbps.
2. With 256-byte packet size, drops occur at 11.1 Mbps.
3. With 512-byte packet size, drops are seen at 22.94 Mbps.
4. With 1400-byte packet size, drops are seen at 47.02 Mbps.

Workaround: There is currently no known workaround.

- CSCsg96864

Description: A Cisco router running the Cisco GGSN Release 7.0 software exhibits the following incorrect behavior when a protocol error is received in a CCA.

- a. When CCFH=terminate, and the protocol error is received in a CCA(Initial) and the subsequent CCA(Final), the PDP context is not deleted.
- b. Upon receipt of protocol errors 3002 and 3005, the GGSN does not failover to a second server.
- c. When CCFH=continue, and the protocol error is received in a CCA(Initial), the PDP context is converted to postpaid, but the create PDP context response is not sent.

Workaround: There is currently no known workaround.

- CSCsh34182

Description: A Cisco GGSN responds to out-of-order GTP packets from the CSG for non-existent PDP contexts with a cause code of 201. This condition does not affect the correct functioning of the system, and occurs only when the CSG is experiencing periods of overload.

Workaround: There is currently no known workaround.

Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.4(9)XG1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek53232

Description: A Cisco MWAM processor crashes during bootup. This condition occurs during periods of high CPU from large amounts of information being printed on the processor (for example, when there is a lot of unsupported configuration), or when traffic is being sent while the processor is booting up.

- CSCsg70355

Description: Starting calendar year 2007, daylight savings summer-time rules might cause Cisco IOS to generate timestamps (such as in syslog messages) that are off by one hour.

By default, the Cisco IOS configuration clock summer-time zone recurring command uses United States standards for daylight savings time rules. The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changes the start date from the first Sunday of April to the second Sunday of March, and it changes the end date from the last Sunday of October to the first Sunday of November.

- CSCsg73514

Description: If the value of the SGSN PLMN-ID is not received from the SGSN, or is invalid, then the “sGSNPLMNIdentifier” information element (IE) with a value of “000000” is included in the ServiceRecord when it should be omitted from the ServiceRecord like it is with G-CDRs.

This condition occurs only if the value for the RAT type is valid and the value for the PLMN ID field is wrong. If the values for both the RAT type and PLMN ID fields are invalid, the ServiceRecord IE is processed correctly.

- CSCsg83911

Description: When the Cisco GGSN generates a Diameter server “Up/Down” trap, the value for the Local ID field is missing when the name that was configured for the Diameter origin host should be used.

- CSCsg92377

Description: Packet drops due to interface throttles are seen on the Cisco GGSN running the release 7.0 image. These throttles occur when bi-directional traffic of 70 Mbps, in the ratio of 1:4 upstream:downstream, is sent for over 60,000 IPv4 PDPs across 500 VRF APNs.

- CSCsg94642

Description: The following SNMP MIBs are not functioning properly:

- cgrprAccPtRevUpstreamTrafficVol.4 = 1339050544120284
- cgrprAccPtRevDownstrTrafficVol.4 = 5272506148764497

- CSCsh18174

Description: When a create PDP context request with a static MS address that matches the ms-address of an already active PDP context on the GGSN is received, the GGSN deletes the existing PDP, and the newer PDP becomes the active PDP context.

This condition occurs only when a create PDP context request with a static ms-address that matches the ms-address of an already existing PDP context on the GGSN. The correct behavior would be for a duplicate IP address check to occur on the GGSN, and for a reject response to be sent to the SGSN for the offending create PDP context request.

- CSCsh18222

Description: The DHCP lease values are invalid/wrong on the standby GGSN when create PDP context update is received on the GGSN for a PDP that is created on an APN on which DHCP addressing is configured.

This condition occurs only when a create PDP context update is received on the GGSN.

- CSCsh20946

Description: An MWAM processor running as Cisco GGSN in a GTP-SR configuration might encounter a software exception during a failover.

This exception occurs with the following condition:

- Approximately 20,000 IPv4 PDP contexts are created on the GGSN processor.
- The MWAM on which the active GGSN resides is reset.
- The Standby GGSN (on the MWAM in the other chassis) becomes the active GGSN.
- The MWAM that was reset boots up, and the GGSN on that MWAM, now functioning as the standby GGSN, tries to synchronize the PDP contexts.

- CSCsh21101

Description: The Cisco GGSN does not take into account the time that has elapsed when it reclaims an IP address which was still in a “hold” state. This condition occurs when DHCP is allocating the IP address and the session is torn down and brought back up just before the renewal 2 to 3 times.

Caveats—Cisco IOS Release 12.4(9)XG

This section documents possible unexpected behavior by Cisco IOS Release 12.4(9)XG and describes only severity 1 and 2 caveats and select severity 3 caveats.

The following caveats are open in Cisco IOS Release 12.4(9)XG, Cisco GGSN Release 7.0.

- CSCek53725

Description: While opening of 8,000 PPP Regen PDPs at 20cps on Cisco GGSN running the release 7.0 image, high CPU (more than 70%) is noticed when the number of opened sessions is close to 8000.

Workaround: There is currently no known workaround.

- CSCek54447

Description: When sending intermediate rate of data packets for all opened 8000 PPP Regen PDP contexts, the CPU is more than 90% on the Cisco GGSN running the release 7.0 image.

Workaround: There is currently no known workaround.

- CSCek54782

Description: During periods of a high rate of create/delete IP PDP contexts with the SGSN sending different restart counters, the Cisco GGSN running the release 7.0 image begins to experience some hanging mobile sessions. These hanging mobile sessions can be deleted by issuing the **clear** command from the GGSN. This condition rarely occurs.

Workaround: There is currently no known workaround.

- CSCek60324

Description: The GGSN quota interface to the CSG fails and the GGSN becomes nonfunctional for a few minutes. This condition occurs when low quota validity (for example, 60) is configured and a medium load (6,000 PDPs) with low traffic exists.

Workaround: There is currently no known workaround. If possible, avoid assigning low quota validity.

- CSCek61309

Description: During periods of overload conditions, the Cisco GGSN experiences a hanging SWIDB. This condition occurs during periods of heavy overload conditions, during which there is a mixture of IPv4 and IPv6 PDP contexts and the IPv6 sessions are close to twice the supported values.

Workaround: There is currently no known workaround.

- CSCse49217

Description: The Cisco GGSN, running the release 7.0 image, does not send a delete notification message to the Cisco IOS SLB when a PDP context is rejected because there is no memory available.

Workaround: There is currently no known workaround.

- CSCsf25506

Description: The Cisco GGSN sends an Accounting Stop message with the cause value as “Lost Carrier.” This condition occurs when the PDP context type is PPP PDP or PPP Regen.

Workaround: There is currently no known workaround.

- CSCsg03663

Description: The Cisco GGSN sends periodic router advertisements (RAs) for IPv6 PDP contexts at the default interval of 200 seconds instead of the interval configured on the base virtual template.

Workaround: There is currently no known workaround.

- CSCsg18574

Description: A couple of issues exist in the way the GGSN security feature is working when CEF is enabled (**ip cef** command) in the process path.

- a. Source address verification

When CEF is enabled, the CEF drop count is not incremented in the **show gprs gtp pdp tid** command output. The **cef_drop** count, **rcv_pkt_count**, and **rcv_bytes_count** counters are not incremented, as well as the corresponding counters displayed by the **show gprs access-point** and **show gprs gtp statistics** commands that reflect how much the GGSN received from the SGSN.

When CEF is disabled, for source addressing the user is being charged. Also, for GTPv1 PDP contexts, 70 bytes of data is being sent, but the **show gprs gtp pdp tid** and **show gprs access-point statistics** commands display the byte count as 74.

- b. Destination address verification

When CEF is enabled, the user is not charged when they should be. The **cef_drop** count, **rcv_pkt_count**, and **rcv_bytes_count** counters are not incremented, as well as the corresponding counters displayed by the **show gprs access-point** and **show gprs gtp statistics** commands that reflect how much the GGSN received from the SGSN in the upstream.

When CEF is disabled, for GTPv1 PDP contexts, 70 bytes of data is being sent, but the **show gprs gtp pdp tid** and **show gprs access-point statistics** commands display the byte count as 74.

- c. Redirect intermobile

When CEF is not enabled, the GGSN sends an ICMP redirect message to the MS. When CEF is enabled, no message is sent.

- d. Redirect all

No ICMP redirect is sent back to the MS with or without CEF enabled.

- CSCsg76357

Description: When the object `cgprsAccPtPdpInServicePolicyName` is set to a value, the resulting configuration on the GGSN may be incorrect. Also, a “get” on this object might not return any value. When deconfigured, spurious access may be seen. This condition occurs when the `cgprsAccPtPdpInServicePolicyName` is set to a value.

Workaround: There is currently no known workaround.

- CSCsg76515

Description: The Cisco GGSN might throw spurious memory errors and reload while unconfiguring the service-policy under the APN and policy maps through SNMP.

Workaround: There is currently no known workaround.

- CSCsf99319

Description: The `show ip local pool` command output, without a pool name, may have an empty line as the first line.

Workaround: There is currently no known workaround.

Cisco MWAM Caveats—Cisco IOS Release 12.4 XG

This section lists the Cisco MWAM caveats that are open and resolved with the Cisco GGSN Release 7.0, Cisco Release 12.4 XG releases.

Caveats—with Cisco IOS Release 12.4(9)XG5

This section contains the following types of Cisco MWAM caveats as they apply to the Cisco GGSN Release 7.0, Cisco IOS Release 12.4(9)XG5 maintenance release:

- [Open Caveat, page 41](#)
- [Resolved Caveats, page 41](#)

Open Caveat

The following caveat is open with Cisco IOS Release 12.4(9)XG5.

- CSCeh82887

Description: When booting multiple MWAMs on the chassis, the link status traps conveying Up, Down are sometimes seen in a different order for each module.

Workaround: There is currently no known workaround.

Resolved Caveats

The following caveats are resolved with Cisco IOS Release 12.4(9)XG3.

- CSCsh86354

Description: The Cisco MWAM processor reloads when all the VTY lines are used and a command is executed on the supervisor remotely using the MWAM Remote Console and Logging (RCAL) feature.

The output of the command does not display on the supervisor console. Instead, the output is printed on the MWAM processor console, and after the display is complete, the MWAM processor reloads.

This condition occurs when all the VTY lines are in use. If only a few are in use, then the RCAL feature works as designed and the output is displayed on the supervisor console.

- CSCsi01197

Description: Executing a command on a Cisco MWAM processor remotely from the supervisor (using the execute-on command, Remote Console and Logging [RCAL] feature) causes packet buffer leak on the processor. Memory from middle buffer pool allocated for this is not released.

This buffer leak occurs when commands are executed remotely from the supervisor on the MWAM processor using the **execute-on** command.

Caveats—with Cisco IOS Release 12.4(9)XG3

This section contains the following types of Cisco MWAM caveats as they apply to the Cisco GGSN Release 7.0, Cisco IOS Release 12.4(9)XG3 maintenance release:

- [Open Caveat, page 41](#)
- [Resolved Caveats, page 41](#)

Open Caveat

The following caveat is open with Cisco IOS Release 12.4(9)XG3.

- CSCeh82887

Description: When booting multiple MWAMs on the chassis, the link status traps conveying Up, Down are sometimes seen in a different order for each module.

Workaround: There is currently no known workaround.

Resolved Caveats

The following caveats are resolved with Cisco IOS Release 12.4(9)XG3.

- CSCsh86354

Description: The Cisco MWAM processor reloads when all the VTY lines are used and a command is executed on the supervisor remotely using the MWAM Remote Console and Logging (RCAL) feature.

The output of the command does not display on the supervisor console. Instead, the output is printed on the MWAM processor console, and after the display is complete, the MWAM processor reloads.

This condition occurs when all the VTY lines are in use. If only a few are in use, then the RCAL feature works as designed and the output is displayed on the supervisor console.

- CSCsi01197

Description: Executing a command on a Cisco MWAM processor remotely from the supervisor (using the execute-on command, Remote Console and Logging [RCAL] feature) causes packet buffer leak on the processor. Memory from middle buffer pool allocated for this is not released.

This buffer leak occurs when commands are executed remotely from the supervisor on the MWAM processor using the **execute-on** command.

Caveats—with Cisco IOS Release 12.4(9)XG2

This section contains the following types of Cisco MWAM caveats as they apply to the Cisco GGSN Release 7.0, Cisco IOS Release 12.4(9)XG2 maintenance release:

- [Open Caveats, page 42](#)
- [Resolved Caveats, page 43](#)

Open Caveats

The following caveats are open with Cisco IOS Release 12.4(9)XG2.

- CSCee49429

Description: When you reset several MWAM modules, a few of them might go to a PowerDown state with the:

```
%C6KPWR-SP-X-DISABLED: power to module in slot 5 set off (Module Failed SCP dnld)
```

message on the supervisor engine console.

Workaround: Power enable the module with the **hw-module module module-number reset** command. If it does not enable the card, issue the **power enable module module-number** command while in configuration mode.

- CSCef76954

Description: The session from the supervisor engine to the SiByte processor on the MWAM is lost if the **no ip routing** command is executed and a default gateway is configured on the processor.

This condition occurs only when IP routing and a default gateway are configured and the **no ip routing** command is executed.

Workaround: Log into the processor control (PC) complex on the MWAM and reset the processor.

- CSCeh47418

Description: While remotely executing commands on the MWAM processors from the supervisor engine, a debuginfo file might be written to the supervisor engine bootflash and the remote console operation might abort. If this condition occurs, memory fragmentation, malloc failure messages, and tracebacks might also be seen.

This condition occurs when the output of the remote command operation is very large.

Workaround: Possible alternatives that can be used include the following:

- Execute the **remote** command for each processor individually instead of using the **execute-on** command with the all keyword option.
- Log onto the MWAM processors individually and execute the **show** commands for which the output is too large for remote execution.

- c. Direct the output of **remote** command from the MWAM onto a management VLAN over the switch fabric (Gig0/0 interface) instead of the EOBC interface.
- CSCeh82887

Description: When booting multiple MWAMs on the chassis, the link status traps conveying Up, Down are sometimes seen in a different order for each module.

Workaround: There is currently no known workaround.
- CSCsf27621

Description: When using the **execute-on** command to an MWAM processor, the supervisor engine returns an error in the format of:

```
%Command to slot <slot> cpu <MWAM processor number> already busy, retry later
```

This condition happens randomly and a processor might stay in the same state for days. There is no command pending for execution to the affected MWAM processor, even though the **show logging slot** command shows the affected processors have “command-Active:Yes” at the same time.

Workaround: Reset the entire MWAM.
- CSCsg06820

Description: The **upgrade rom-monitor** command displays an “ambiguous error” when the **invalidate** keyword option is not specified, even though the **invalidate** keyword option is the only **upgrade rom-monitor** command option.

Workaround: Specify the **upgrade rom-monitor** command with the **invalidate** keyword option.
- CSCsg10969

Description: The Cisco GGSN running on an MWAM processor completely lose its configuration when certain conditions occur. This loss occurs when the processor is in local configuration mode, the GGSN Release 7.0 image is loaded with the GGSN Release 7.0 configuration and then the image is changed to a GGSN Release 6.0 image, and the configuration is saved by issuing the **write memory** command.

Workaround: Do not switch between GGSN Release 6.0 and Release 7.0 images from local-config mode and download the startup configuration via TFTP.

Resolved Caveats

There have been no Cisco MWAM caveats resolved for Cisco IOS Release 12.4(9)XG2.

Caveats—with Cisco IOS Release 12.4(9)XG1

This section contains the following types of Cisco MWAM caveats as they apply to the Cisco GGSN, Cisco IOS Release 12.4(9)XG1 maintenance release:

- [Open Caveats, page 44](#)
- [Resolved Caveats, page 45](#)

Open Caveats

The following caveats are open with Cisco IOS Release 12.4(9)XG1.

- CSCee49429

Description: When you reset several MWAM modules, a few of them might go to a PowerDown state with the:

```
%C6KPWR-SP-X-DISABLED: power to module in slot 5 set off (Module Failed SCP dnld)
```

message on the supervisor engine console.

Workaround: Power enable the module with the **hw-module module *module-number* reset** command. If it does not enable the card, issue the **power enable module *module-number*** command while in configuration mode.

- CSCef76954

Description: The session from the supervisor engine to the SiByte processor on the MWAM is lost if the **no ip routing** command is executed and a default gateway is configured on the processor.

This condition occurs only when IP routing and a default gateway are configured and the **no ip routing** command is executed.

Workaround: Log into the processor control (PC) complex on the MWAM and reset the processor.

- CSCeh47418

Description: While remotely executing commands on the MWAM processors from the supervisor engine, a debuginfo file might be written to the supervisor engine bootflash and the remote console operation might abort. If this condition occurs, memory fragmentation, malloc failure messages, and tracebacks might also be seen.

This condition occurs when the output of the remote command operation is very large.

Workaround: Possible alternatives that can be used include the following:

- Execute the **remote** command for each processor individually instead of using the **execute-on** command with the all keyword option.
 - Log onto the MWAM processors individually and execute the **show** commands for which the output is too large for remote execution.
 - Direct the output of **remote** command from the MWAM onto a management VLAN over the switch fabric (Gig0/0 interface) instead of the EOBC interface.
- CSCeh82887

Description: When booting an MWAM, Admin Down messages are received for the internal interfaces Gig8/1, Gig8/2, Gig8/3 for the MWAM on slot 8. These interfaces are internal interfaces that cannot be configured by the user for disabling traps. Therefore the interfaces should be always shown as Admin Up, and Admin down traps should not be sent.

Additionally, when booting different MWAMs on the chassis, the link status traps conveying Up, Down, and Admin Down (which should not be seen) are seen coming in different order for each module. These traps are seen for the internal interface of each MWAM when the MWAM is reset.

Workaround: There is currently no known workaround.

- CSCse36277

Description: The MWAM is unable to see the supervisor engine as its CDP neighbor. This condition occurs when CDP is enabled on the subinterfaces of the MWAM. While the MWAM is unable to see the supervisor engine as its CDP neighbor, the MWAM subinterface is seen in the supervisor engine's CDP neighbor table.

Workaround: Enable CDP on the main interface, not the subinterfaces.

- CSCsf27621

Description: When using the **execute-on** command to an MWAM processor, the supervisor engine returns an error in the format of:

```
%Command to slot <slot> cpu <MWAM processor number> already busy, retry later
```

This condition happens randomly and a processor might stay in the same state for days. There is no command pending for execution to the affected MWAM processor, even though the **show logging slot** command shows the affected processors have “command-Active:Yes” at the same time.

Workaround: Reset the entire MWAM.

- CSCsg06820

Description: The **upgrade rom-monitor** command displays an “ambiguous error” when the **invalidate** keyword option is not specified, even though the **invalidate** keyword option is the only **upgrade rom-monitor** command option.

Workaround: Specify the **upgrade rom-monitor** command with the **invalidate** keyword option.

- CSCsg10969

Description: The Cisco GGSN running on an MWAM processor completely lose its configuration when certain conditions occur. This loss occurs when the processor is in local configuration mode, the GGSN Release 7.0 image is loaded with the GGSN Release 7.0 configuration and then the image is changed to a GGSN Release 6.0 image, and the configuration is saved by issuing the **write memory** command.

Workaround: Do not switch between GGSN Release 6.0 and Release 7.0 images from local-config mode and download the startup configuration via TFTP.

Resolved Caveats

There have been no Cisco MWAM caveats resolved for Cisco IOS Release 12.4(9)XG1.

Caveats—with Cisco IOS Release 12.4(9)XG

This section contains the following types of Cisco MWAM caveats as they apply to the Cisco GGSN, Cisco IOS Release 12.4(9)XG maintenance release:

- [Open Caveats, page 46](#)
- [Resolved Caveats, page 47](#)

Open Caveats

The following caveats are open with Cisco IOS Release 12.4(9)XG.

- CSCee49429

Description: When you reset several MWAM modules, a few of them might go to a PowerDown state with the:

```
%C6KPWR-SP-X-DISABLED: power to module in slot 5 set off (Module Failed SCP dnld)
```

message on the supervisor engine console.

Workaround: Power enable the module with the **hw-module module *module-number* reset** command. If it does not enable the card, issue the **power enable module *module-number*** command while in configuration mode.

- CSCef76954

Description: The session from the supervisor engine to the SiByte processor on the MWAM is lost if the **no ip routing** command is executed and a default gateway is configured on the processor.

This condition occurs only when IP routing and a default gateway are configured and the **no ip routing** command is executed.

Workaround: Log into the processor control (PC) complex on the MWAM and reset the processor.

- CSCeh47418

Description: While remotely executing commands on the MWAM processors from the supervisor engine, a debuginfo file might be written to the supervisor engine bootflash and the remote console operation might abort. If this condition occurs, memory fragmentation, malloc failure messages, and tracebacks might also be seen.

This condition occurs when the output of the remote command operation is very large.

Workaround: Possible alternatives that can be used include the following:

- Execute the **remote** command for each processor individually instead of using the **execute-on** command with the all keyword option.
 - Log onto the MWAM processors individually and execute the **show** commands for which the output is too large for remote execution.
 - Direct the output of **remote** command from the MWAM onto a management VLAN over the switch fabric (Gig0/0 interface) instead of the EOBC interface.
- CSCeh82887

Description: Upon booting an MWAM, Admin Down messages are received for the internal interfaces Gig8/1, Gig8/2, Gig8/3 for the MWAM on Slot 8. These interfaces are internal interfaces that cannot be configured by the user for disabling traps. Therefore the interfaces should be always shown as Admin Up, and Admin down traps should not be sent.

Additionally, on booting different MWAMs on the chassis, the link status traps conveying Up, Down (and Admin Down which should not be seen) are seen coming in different order for each module.

These traps are seen for the internal interface of each MWAM when the MWAM is reset.

Workaround: There is currently no known workaround.

- CSCse36277

Description: The MWAM is unable to see the supervisor engine as its CDP neighbor. This condition occurs when CDP is enabled on the subinterfaces of the MWAM. The MWAM is unable to see the supervisor engine as its CDP neighbor, however, the MWAM subinterface is seen in the supervisor engine's CDP neighbor table.

Workaround: Enable CDP on the main interface, not the subinterfaces.

- CSCsf27621

Description: When using the **execute-on** command to an MWAM processor, the supervisor engine returns an error in the format of:

```
%Command to slot <slot> cpu <MWAM processor number> already busy, retry later
```

This condition starts happening randomly and a processor may stay in the same state for days. There is no command pending for execution to the affected MWAM processor, even though the **show logging slot** command shows the affected processors have “command-Active:Yes” at the same time.

Workaround: Reset the entire MWAM.

- CSCsg06820

Description: The **upgrade rom-monitor** command displays an “ambiguous error” when the **invalidate** keyword option is not specified, even though the **invalidate** keyword option is the only **upgrade rom-monitor** command option.

Workaround: Specify the **upgrade rom-monitor** command with the **invalidate** keyword option.

- CSCsg10969

Description: The Cisco GGSN running on an MWAM processor completely lose its configuration when certain conditions occur. This loss occurs when the processor is in local configuration mode, the GGSN Release 7.0 image is loaded with the GGSN Release 7.0 configuration and then the image is changed to GGSN Release 6.0, and the configuration is saved by issuing the **write memory** command.

Workaround: Do not switch between GGSN Release 6.0 and Release 7.0 images from local-config mode and download the startup configuration via TFTP.

Resolved Caveats

There have been no Cisco MWAM caveats resolved for Cisco IOS Release 12.4(9)XG.

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 48](#)
- [Platform-Specific Documents, page 48](#)
- [Cisco IOS Software Documentation Set, page 49](#)

Release-Specific Documents

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

- *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720 and Supervisor Engine 2*
- *Cross-Platform Release Notes for Cisco IOS Release 12.4*

On CCO at:

Technical Support and Documentation: Technical Support and Documentation: Cisco IOS Software: Cisco IOS Software Releases 12.4 Mainline: Release Notes: Cross-Platform Release Notes

- *Caveats for Cisco IOS Release 12.4T*

See *Caveats for Cisco IOS Release 12.4* and *Caveats for Cisco IOS Release 12.4T*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.4 and Release 12.4T.

On CCO at:

Technical Support and Documentation: Technical Support and Documentation: Cisco IOS Software: Cisco IOS Software Releases 12.4 T: Release Notes: Cross-Platform Release Notes



Note

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

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

Technical Support and Documentation: Technical Support and Documentation: Cisco IOS Software: Cisco IOS Software Mainline

Platform-Specific Documents

These documents are available for the Catalyst 6500/Cisco 7600 series platforms on Cisco.com and the Documentation CD-ROM:

- *Cisco Multi-Processor WAN Application Module Installation and Configuration Notes*
- Catalyst 6500 Series Switch Documentation:
 - *Catalyst 6500 Series Switch Module Installation Guide*
 - *Catalyst 6500 Series Switch Installation Guide*
 - *Multi-processor WAN Application Module Installation and Configuration Note*
- Cisco 7600 Series Routers Documentation:
 - *Cisco 7600 Series Internet Router Installation Guide*
 - *Cisco 7600 Series Internet Router Module Installation Guide*
 - *Cisco 7609 Internet Router Installation Guide*

Catalyst 6500 Series Switch Documentation is available at the following URL:

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

Cisco 7600 Series Routers Documentation is available at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guides_books_list.html

Cisco IOS Software Documentation Set

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

Documentation Modules

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

On CCO at:

Technical Support and Documentation: Technical Support and Documentation: Cisco IOS Software: Cisco IOS Software Releases 12.4 Mainline: Command References

Technical Support and Documentation: Technical Support and Documentation: Cisco IOS Software: Cisco IOS Software Releases 12.4 Mainline: Configuration Guides



Note

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

Documentation Roadmap for Implementing GGSN Release 6.0 on the Cisco MWAM

The following sections list related documentation (by category and then by task) that will be useful when implementing a Cisco GGSN on the Cisco MWAM platform.

General Overview Documents

Core Cisco 7609 Documents:

http://cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

Navigating from Cisco.com:

Technical Support and Documentation: Technical Support and Documentation: Routers: Cisco 7600 Series Routers

Documentation List by Task

For the most up-to-date list of documentation on the Cisco 7600 series router, refer to the Cisco 7600 Series Routers Documentation Roadmap on Cisco.com at:

http://cisco.com/en/US/products/hw/routers/ps368/products_documentation_roadmap09186a00801ebcd9.html

Getting Started

- *Cisco 7600 Series Internet Router Essentials*
http://cisco.com/en/US/products/hw/routers/ps368/products_quick_start09186a0080092248.html
- *Regulatory Compliance and Safety Information for the Cisco 7600 Series Internet Routers*
<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/rcsi/index.html>

Unpack and install the Cisco 7609 router:

- *Cisco 7609 Internet Router Installation Guide*
http://cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_book09186a008007e036.html

Install the Supervisor module and configure the router (basic configuration—VLANs, IP, etc.) using the following documentation:

- *Cisco 7600 Series Internet Router Module Installation Guide*
http://cisco.com/en/US/products/hw/routers/ps368/products_module_installation_guide_book09186a008007cd9d.html
- Cisco IOS Software Configuration Guide that applies to the latest release at the time of FCS

Install and complete the basic Cisco MWAM configuration:

- *Cisco 7600 Series Internet Router Module Installation Guide*
http://cisco.com/en/US/products/hw/routers/ps368/products_module_installation_guide_book09186a008007cd9d.html
- Cisco Multi-processor WAN Application Module Installation and Configuration Note
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/mwamicn/index.htm>

Download the Cisco IOS software image containing the GGSN feature set and configure the GGSNs on the MWAM:

- Cisco GGSN 7.0 Configuration Guide and Command Reference and Associated Release Notes for Cisco IOS Release 12.4(9)XG.
http://cisco.com/en/US/products/sw/wirelssw/ps873/tsd_products_support_series_home.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.

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, 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 Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, 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. (0910R)

Release Notes for Cisco GGSN Release 7.0 on the Cisco MWAM, Cisco IOS Release 12.4(15)XG5

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