# Release Notes for Cisco GGSN Release 6.0 on the Cisco MWAM, Cisco IOS Software Release 12.4 XB

**Current Publication Date: August 24, 2011**
**Last Publication Date: March 24, 2010**

Cisco IOS Release 12.4(2)XB12

These release notes for the Cisco Gateway GPRS Support Node (GGSN) Release 6.0 on the Cisco Multi-processor WAN Application Module (MWAM) describe the enhancements provided in Cisco IOS Release 12.4(2)XB12. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4(2)XB12, see the "Cisco GGSN Caveats, Cisco IOS Release 12.4 XB" 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

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

- New and Changed Information, page 10
- Cisco GGSN Caveats, Cisco IOS Release 12.4 XB, page 15
- Cisco MWAM Caveats, with Cisco IOS Release 12.4 XB, page 49
- Related Documentation, page 65
- Documentation Roadmap for Implementing GGSN Release 6.0 on the Cisco MWAM, page 67
- Documentation Roadmap for Implementing GGSN Release 6.0 on the Cisco MWAM, page 67


# 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 3


## 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.
- 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(2)XB8 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(2)XB12***

| Platforms | Feature Sets | Software Image | Flash Memory Recommended | DRAM Memory Recommended | Runs From |
|---|---|---|---|---|---|
| **Cisco MWAM on Catalyst 6500 / Cisco 7600** | GGSN Standard Feature Set | c6svc5fmwam-g8is-mz.124-2.XB12.bin | 128MB | 1 GB | RAM |

# Hardware and Software Requirements

Proper implementation of the Cisco GGSN Release 6.0 features in the Cisco IOS Release 12.4(2)XB12 software 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** GGSN Release 5.2, Cisco IOS Release 12.3(14)YQ and later, supports both the standard MWAM 512 MB per processor memory option and the 1 GB per processor memory option.

### GTP Session Redundancy

In addition to the hardware and software requirements listed above, implementing GPRS tunneling protocol (GTP) Session Redundancy (GTP-SR) requires the following:

- Two Cisco 7600 series routers with one of the above supervisor engine configurations.
- At minimum, two Cisco MWAMs—one in each Cisco 7600 series router.
- Hot Standby Router Protocol (HSRP) Version 2.

### Enhanced Service-Aware Billing

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

**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 Internetwork Operating System Software
IOS (tm) MWAM Software (MWAM-g8is-M), Version 12.4(2)XB12, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 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(2)XB12, note 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.

For the Cisco 7200 series router, the following list shows the maximum number of PDP contexts supported on the GGSN according to the memory and Cisco 7206 series router in use when no method of PPP has been configured:

  - Cisco 7206 VXR NPE-300 with 256 Mb RAM—80,000 IP PDP contexts
  - Cisco 7206 VXR NPE-400 router with 512 Mb RAM—135,000 IP PDP contexts

For the Catalyst 6500 series switch/Cisco 7600 series router, the Cisco MWAM can support up to 60,000 IP PDP contexts per GGSN instance, with a maximum of 300,000 IP PDP contexts per MWAM on which five GGSNs 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 module (no direct console).
- Available memory for bootflash 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** global configuration command.
  - To ensure that the HRSP interface does not declare itself active until it is ready to process a peer's Hello packets, configure the delay period before the initialization of HSRP groups with the **standby delay minimum 100 reload 100 interface** configuration command under the HRSP 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** configuration command.

```
!
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:

- GTP-SR is supported on the Cisco 7600 platform only.
- 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 / 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-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*T3 must be greater than:

  2 x RADIUS timeout + *N* x DCCA timeout + 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 XB releases:


- New and Changed Information in Cisco IOS Release 12.4(2)XB12, page 10
- New and Changed Information in Cisco IOS Release 12.4(2)XB11, page 10
- New and Changed Information in Cisco IOS Release 12.4(2)XB10, page 10
- New and Changed Information in Cisco IOS Release 12.4(2)XB9, page 11
- New and Changed Information in Cisco IOS Release 12.4(2)XB8, page 11
- New and Changed Information in Cisco IOS Release 12.4(2)XB7, page 11
- New and Changed Information in Cisco IOS Release 12.4(2)XB6, page 11
- New and Changed Information in Cisco IOS Release 12.4(2)XB5, page 14
- New and Changed Information in Cisco IOS Release 12.4(2)XB4, page 14
- New and Changed Information in Cisco IOS Release 12.4(2)XB3, page 14
- New and Changed Information in Cisco IOS Release 12.4(2)XB2, page 14
- New and Changed Information in Cisco IOS Release 12.4(2)XB1, page 14
- New and Changed Information in Cisco IOS Release 12.4(2)XB, page 15


## New and Changed Information in Cisco IOS Release 12.4(2)XB12

There are no new features in Cisco IOS Release 12.4(2)XB12.

## New and Changed Information in Cisco IOS Release 12.4(2)XB11

There are no new features in Cisco IOS Release 12.4(2)XB11.

## New and Changed Information in Cisco IOS Release 12.4(2)XB10

There are no new features in Cisco IOS Release 12.4(2)XB10.

# New and Changed Information in Cisco IOS Release 12.4(2)XB9

There are no new features in Cisco IOS Release 12.4(2)XB9.

#### Configuring GGSN GTP Session Redundancy

The following restriction has been added to the "Limitations and Restrictions" list in the "Configuring GGSN Session Redundancy" chapter of the Cisco GGSN Release 6.0 Configuration Guide:

- Broadcast accounting is not support with GTP-SR.

**Note** Additionally, broad cast accounting is not supported with wait accounting.

Note that these broad cast accounting restrictions apply to Cisco GGSN Release 6.0, and all prior.

# New and Changed Information in Cisco IOS Release 12.4(2)XB8

There are no new features in Cisco IOS Release 12.4(2)XB8.

# New and Changed Information in Cisco IOS Release 12.4(2)XB7

There are no new features in Cisco IOS Release 12.4(2)XB7.

# New and Changed Information in Cisco IOS Release 12.4(2)XB6

There are no new features in Cisco IOS Release 12.4(2)XB6.

## Amendments and Corrections to the Cisco GGSN Release 6.0 Documentation

The following amendments and corrections will be made to the *Cisco GGSN Release 6.0Configuration 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 read as follows:

- 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}` | Configures the default Credit Control Failure Handling (CCFH) action to take on PDP contexts when a fault condition occurs.<br>• 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.<br>• TERMINATE—Terminates the PDP context and the CC session.<br>• 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.<br>The default is terminate.<br>A value from the DCCA server in a CCA overrides this default. |

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

| Command | Purpose |
|---|---|
| `Router(config-dcca-profile)# ccfh {continue \| terminate \| retry_terminate}` | Configures the default Credit Control Failure Handling (CCFH) action to take on PDP contexts when a fault condition occurs.<br>• **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.<br>• **terminate**—Terminates the PDP context and the CC session.<br>• **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.<br>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.<br>The default is terminate.<br>A value from the DCCA server in a CCA overrides this default. |

The following amendments and corrections will be made to the *Cisco GGSN Release 6.0 Command Reference*:

#### 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.

#### 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 credit control request (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** | 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.<br><br>The DCCA client retries to send the credit control request (CRR) to an alternate server and if a failure-to-send condition occurs with the alternate server, the PDP context is terminated. |

# New and Changed Information in Cisco IOS Release 12.4(2)XB5

There are no new features in Cisco IOS Release 12.4(2)XB5.

# New and Changed Information in Cisco IOS Release 12.4(2)XB4

There are no new features in Cisco IOS Release 12.4(2)XB4.

# New and Changed Information in Cisco IOS Release 12.4(2)XB3

There are no new features in Cisco IOS Release 12.4(2)XB3.

# New and Changed Information in Cisco IOS Release 12.4(2)XB2

The Cisco IOS Release 12.4(2)XB2 release of Cisco GGSN Release 6.0 introduces support for Online Charging Server (OCS) address selection.

For information about the OCS Address Selection feature, see the “Configuring Enhanced Service-Aware Billing” chapter of the Cisco GGSN Release 6.0 Configuration Guide at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xb2/ggsn60_c/ggsnsa.htm

# New and Changed Information in Cisco IOS Release 12.4(2)XB1

There are no new features in Cisco IOS Release 12.4(2)XB1.

## New and Changed Information in Cisco IOS Release 12.4(2)XB

This release of Cisco GGSN Release 6.0 provides support for the following new features:

- GTP Server Load Balancing (SLB) Stickiness
- Proxy Call Session Control Function (P-CSCF) Discovery
- Enhanced MIB Support - Cisco Content Services Gateway (CSG), Diameter Credit Control Application (DCCA), Persistent Storage Device (PSD) Client

For information about the features in GGSN Release 6.0, see the Cisco IOS Release 12.4(2)XB Cisco GGSN Release 6.0 configuration guide and command reference at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xb2/index.htm

# Cisco GGSN Caveats, Cisco IOS Release 12.4 XB

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.

This section contains the following caveat information:


- Caveats—Cisco IOS Release 12.4(2)XB12, page 16
- Caveats—Cisco IOS Release 12.4(2)XB11, page 17
- Caveats—Cisco IOS Release 12.4(2)XB10, page 19
- Caveats—Cisco IOS Release 12.4(2)XB9, page 20
- Caveats—Cisco IOS Release 12.4(2)XB8, page 21
- Caveats—Cisco IOS Release 12.4(2)XB7, page 22
- Caveats—Cisco IOS Release 12.4(2)XB6, page 23
- Caveats—Cisco IOS Release 12.4(2)XB5, page 27
- Caveats—Cisco IOS Release 12.4(2)XB4, page 30
- Caveats—Cisco IOS Release 12.4(2)XB3, page 30
- Caveats—Cisco IOS Release 12.4(2)XB2, page 35
- Caveats—Cisco IOS Release 12.4(2)XB1, page 40
- Caveats—Cisco IOS Release 12.4(2)XB, page 45


All caveats in Cisco IOS Release 12.4 and Cisco IOS Release 12.4 T are also in Cisco IOS Release 12.4(2)XB6.

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

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.

**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.

# Caveats—Cisco IOS Release 12.4(2)XB12

The following caveats are open or resolved in Cisco IOS Release 12.4(2)XB12.

## Open Caveat

There are no known caveats open in the Cisco IOS Release 12.4(2)XB12, Cisco GGSN Release 6.0 image.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB12.

- CSCso02147

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCso85193

  After running for some time, the Cisco 7609 generates a general error when setting a value on any SNMP object. The **show users** command indicates a ghost entry:

  ```
  #show users
  Line User Host(s) Idle Location
  1 vty 0 Virtual Exec 00:00:00
  ```

  This condition occurs on routers running Cisco IOS Release 12.2(33)SRB2 on the supervisor engine module.

- CSCsy70508

  When DHCP addressing is used, the standby GGSN has a fewer number of sessions than the active GGSN. As PDP contexts are created and deleted, the standby GGSN deletes some active sessions in error. This condition results in fewer number of active sessions on the standby GGSN than on the active GGSN.

- CSCsx18115

  Service-aware PDP contexts might remain in memory after the call is released. This condition might occur for service-aware PDPs during periods of high stress conditions (>99% CPU) that continue for several hours.

- CSCta15966

  During periods of high stress conditions (>99% CPU) that last for several hours, a service-aware PDP might remain in memory after the call is released.

- CSCtb49987

  The number of IP addresses allocated does not match in the active and standby GGSN. The numbers on the active GGSN are correct.

- CSCti07086

  When IP address allocation is configured using local pools, sometimes the active-standby GGSN pairs are out of sync. Once this condition occurs, the standby does not following the active GGSN.

  This condition occurs when the **ip local pool** command is configured with the **group** keyword option specified (for example **ip local pool mypool 1.1.1.1 1.1.1.255 group mygroup**).

- CSCti48483

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtn14284

  An AAA access-request returns with an internal error, and on the Cisco GGSN the following unconditional bug information is printed: “AAA had an unexpected return.”

  This condition occurs when an access-request is sent to the AAA server during periods of stress conditions on the client process and a failure to build the RADIUS packet occurs.

# Caveats—Cisco IOS Release 12.4(2)XB11

The following caveats are open, resolved, or closed in Cisco IOS Release 12.4(2)XB11.

## Open Caveat

There are no known caveats open in the Cisco IOS Release 12.4(2)XB11, Cisco GGSN Release 6.0 image.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB11.

- CSCsr11468

  On the Cisco GGSN, if memory is depleted, and if the SLB next hop address is set by Simple Network Management Protocol (SNMP) command, a memory issue might occur.

- CSCtb77620

  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 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 over with GTPv1.

- CSCtc07857

  A fatal error occurs with GPRS tunneling protocol (GTP) parsing of PPP.

- CSCtb93855

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml.

- CSCsv06714

  When the Cisco GGSN receives a Credit Control Answer (CCA) with a result code of 5012 for a service, the GGSN does not process the CCA correctly. The GGSN keeps service waiting for CCA state, and does not send a response to the Cisco CSG2.

- CSCsv11128

  If the User Location Info information element (IE) is not received in a Create PDP Context request, the GGSN does not include the USER-LOCATION-INFO attribute value pair (AVP) when it requests quota for prepaid services. This condition occurs when the User Location Info IE is not received in a Create PDP Context request, even though the Routing Area Identity (RAI) is included.

## Closed Caveat

The following caveat has been closed in Cisco IOS Release 12.4(2)XB11.

- CSCse49217

  **Description:** The Cisco GGSN does not send a delete notification message to the Cisco IOS SLB when the PDP context is rejected because no memory is available.

# Caveats—Cisco IOS Release 12.4(2)XB10

The following caveats are open and resolved in Cisco IOS Release 12.4(2)XB10.

## Open Caveat

The following caveat is open in the Cisco IOS Release 12.4(2)XB10, Cisco GGSN Release 6.0 image.

- CSCse49217

  **Description:** The Cisco GGSN does not send a delete notification message to the Cisco IOS SLB when the PDP context is rejected because no memory is available.

  **Workaround:** There is currently no known workaround.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB10.

- CSCek67305

  **Description:** The vaccess for an access point name (APN) has no IP address. This is a very rare condition that occurs under the following conditions:

  - An APN is configured with a DHCP server that is assigning IP addresses.
  - A high number of PDP contexts are deleted followed by these PDP being created within 5 seconds.
  - The above is repeated, and the vaccess for this APN loses its IP address.

- CSCsj85065

  A Cisco IOS device may crash while processing an Secure Sockets Layer (SSL) packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

  Cisco has released free software updates that address this vulnerability.

  Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

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

- 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.

- CSCsk62253

  Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

  1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
  2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml

- 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.

- 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.

# Caveats—Cisco IOS Release 12.4(2)XB9

The following caveats are open and resolved in Cisco IOS Release 12.4(2)XB9.

## Open Caveats

There are no known caveats open in the Cisco IOS Release 12.4(2)XB9, Cisco GGSN Release 6.0 image.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB9.

- CSCsf97873

  **Description:** On an APN enabled for PPP regeneration, creating a Layer 2 Tunneling Protocol (L2TP) from the GGSN to the 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.

- 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.

# Caveats—Cisco IOS Release 12.4(2)XB8

The following caveats are open and resolved in Cisco IOS Release 12.4(2)XB8.

## Open Caveats

There are no known caveats open in the Cisco IOS Release 12.4(2)XB8, Cisco GGSN Release 6.0 image.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB8.

- CSCsg91306

  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.

- 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.

# Caveats—Cisco IOS Release 12.4(2)XB7

The following caveats are open and resolved in Cisco IOS Release 12.4(2)XB7.

## Open Caveats

There are no known caveats open in the Cisco IOS Release 12.4(2)XB7 Cisco GGSN Release 6.0 image.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB7.

- CSCir02107

  **Description:** With redundantly-configured Cisco GGSNs, when a path is created without a recovery IE having been received from the SGSN, and then the path is updated with a valid recovery IE, the standby GGSN does not update the recovery IE with the new value.

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

- 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.

# Caveats—Cisco IOS Release 12.4(2)XB6

The following caveats are open and resolved in Cisco IOS Release 12.4(2)XB6.

## Open Caveats

There are no known caveats open in the Cisco IOS Release 12.4(2)XB6 Cisco GGSN Release 6.0 image.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB6.

- 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.

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml

- CSCir01528

  **Description:** On a Cisco GGSN, configured to allocate IP addresses from a RADIUS server for an APN, there can be an incorrect syslog message printed when the RADIUS server does not return an IP address for a particular user. This condition occurs only when the RADIUS server is used for address allocation and the server does not return an IP address for a particular user. The message incorrectly indicates that no RADIUS server is available.

- CSCsd14568

  **Description:** One might not be able to query the redundancy statistics MIB objects without having service-aware functionality enabled (the **gprs service-aware** global configuration command).

- CSCsd81407

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- 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.

- CSCse68355

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsf18925

  **Description:** On a Cisco MWAM running the Cisco GGSN software, the processor might reload while doing multiple SNMP operations on a service-aware APN. The reload rarely occurs and is difficult to recreate. This condition occurs only if service-aware functionality is configured, and multiple SNMP operations are being performed at the same time.

- CSCsg18574

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

  a. Source address verification—When CEF is enabled, the cef_drop count, rcv_pkt_count, and rcv_bytes_count counters are not incremented in the **show gprs gtp pdp tid** command output, 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, when source address verification is enabled, 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.

- CSCsg83347

  **Description:** Objects cgprsAccPtName and cgprsAccPtMsIsdnSuppressedValue might not accept a null string.

- CSCsg91326

  **Description:** When the Diameter server experiences delays in responses and the Cisco GGSN keeps generating new authorization requests, the Gi0/0 interface on MWAM shows the input queue size increase to the maximum value. This causes GGSN to encounter a path failure to the SGSN and active PDP's are deleted. This condition occurs when the Diameter server delays the responses.

- CSCsg94642

  **Description:** The following SNMP MIBs are not functioning properly:

  – cgprsAccPtRevUpstreamTrafficVol.4 = 1339050544120284

  – cgprsAccPtRevDownstrTrafficVol.4 = 5272506148764497

- 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.

- CSCsh87457

  **Description:** After setting cgprsAccPtName to null through SNMP, the following conditions might occur:

  – The APN name might display with some junk characters in the running configuration.

  – The Cisco GGSN might reload when the APN name is changed using the CLI.

- 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.

- CSCsi60004

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsi80749

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsj40311

  **Description:** The Cisco GGSN, might reload when a create PDP context request is received with an extension header to the GTP header and the extension header has length of 0 bytes. This circumstance rarely occurs.

- CSCsj51090

  **Description:** When a redundant GGSN configuration exists, after a switchover, the newly active GGSN cannot forward traffic on PDPs that belong to some access points. This condition occurs only after a switchover from an active to a standby GGSN and only on a few APNs.

- CSCsj74145

  **Description:** On a Cisco MWAM running the Cisco GGSN software, if an Error-Indication is received from the SGSN on a GTPv1 path, which leads to a PDP context deletion on the GGSN, the corresponding Accounting-Stop, will have the Acct-Terminate-Cause as "Unknown" instead of "Nas-Error." This would be Nas-Error if the SGSN path is GTPv0. This Error-Indication is received on a GTPv1 path.

# Caveats—Cisco IOS Release 12.4(2)XB5

The following caveats are open and resolved in Cisco IOS Release 12.4(2)XB5.

## Open Caveat

The following caveat is open in the Cisco IOS Release 12.4(2)XB5, Cisco GGSN Release 6.0 image.

- CSCej21472

  **Description:** In Cisco IOS GGSN Release 6.0, when an extended QoS profile is sent to the GGSN, the debugs do not correctly display the QoS profile. Octets 15 and 16 of the extended QoS IE show incorrect values for the extended maximum and guaranteed bit rates for downlink.

  This condition occurs when an extended QoS IE is sent in a create PDP context request.

  **Workaround:** There is currently no known workaround.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB5.

- 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.

- CSCej20505

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCir00690

  **Description:** When the Cisco GGSN sends Diameter packets that include a Radio Access Technology value, the M-bit is not set although it should be.

- CSCir00864

  **Description:** The Cisco GGSN encodes an IPv4 Proxy Call Session Control Functions (P-CSCF) address as an IPv4 container inside the Protocol Control Option (PCO) element (IE) when, according to TS 24.008, the Cisco GGSN should encode an IPv4 P-CSCF address as an IPv6 mapped address (defined in RFC 2373).

- CSCse83529

  **Description:** Encoding of the quota push is incorrect, therefore, the PDP is kept in a PENDING_QP because no GTP response sent back to the SGSN.

  This condition occurs when the Diameter server is configured with a category ID (4292967295) for a rule base ID (ABC), and a GTPv0 PDP context request is sent to a prepaid APN. The Cisco GGSN sends a CCR request and receives a CCA initial response with the category ID. The GGSN attempts to encode a quota push request to the CSG, but according to the log, it is not encoding a complete quota push with this category ID. The category state is changed to PENDING_QP. The service ID is displayed as “Empty” in the **show gprs gtp pdp tid service all** command output.

- CSCsf13403

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

- CSCsf30058

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)

  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCsg16908

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The Cisco IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the Cisco IOS FTP Client feature.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

- CSCsg41346

  **Description:** The Cisco GGSN, in a GTP session redundancy configuration, is unable to send GTP IMSI sticky delete notifications to the GTP SLB after a failover. The GTP IMSI sticky delete notifications fail only when the PDP is deleted after a standby-to-active GGSN switchover. Without a switchover, the GTP IMSI sticky delete notification from the GGSN to the SLB is successful.

- CSCsh18222

  **Description:** The DHCP lease values are invalid on the Standby GGSN when a Create as an Update request is received on the GGSN for a PDP.

- 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(2)XB4

The following caveats are open, resolved, and closed in Cisco IOS Release 12.4(2)XB4.

## Open Caveat

The following caveat is open in the Cisco IOS Release 12.4(2)XB4, Cisco GGSN Release 6.0 image.

- CSCej21472

  **Description:** In Cisco IOS GGSN Release 6.0, when an extended QoS profile is sent to the GGSN, the debugs do not correctly display the QoS profile. Octets 15 and 16 of the extended QoS IE show incorrect values for the extended maximum and guaranteed bit rates for downlink.

  This condition occurs when an extended QoS IE is sent in a create PDP context request.

  **Workaround:** There is currently no known workaround.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB4.

- CSCin99850

  **Description:** The Cisco GGSN crashes when the **show gprs gtp pdp tid tid** command is executed during a period of multiple PDP creates and deletes.

- CSCse62599

  **Description:** A Cisco GGSN reloads when rare passwords are used. This reload occurs when the create PDP context request uses the virtual APN feature and the password has the "@password" character.

# Caveats—Cisco IOS Release 12.4(2)XB3

The following caveats are open, resolved, and closed in Cisco IOS Release 12.4(2)XB3.

## Open Caveat

The following caveat is open in the Cisco IOS Release 12.4(2)XB3, Cisco GGSN Release 6.0 image.

- CSCej21472

  **Description:** In Cisco IOS GGSN Release 6.0, when an extended QoS profile is sent to the GGSN, the debugs do not correctly display the QoS profile. Octets 15 and 16 of the extended QoS IE show incorrect values for the extended maximum and guaranteed bit rates for downlink.

  This condition occurs when an extended QoS IE is sent in a create PDP context request.

  **Workaround:** There is currently no known workaround.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB3.

- CSCei59800

  **Description:** When a view definition with "commands configured include all policy-map" included is configured, a view user is not able to configure the submode commands under the policy-map.

- CSCek37616

  **Description:** An additional attribute, CC-tariff-change-units, is sent in the CCR(Update) message to the Diameter server with value of "units-indeterminate" when a SERVICE-REAUTH message is received from CSG after a Tariff-Time change.

  This condition occurs with the following:

  a. The PDP context is service aware.
  b. A Tariff-Time change event occurs for services associated with the PDP context and a CCR(Update) is sent to the Diameter server.
  c. Quota is allocated to the service by Diameter server in a CCA(Update) message.
  d. Another Service-Reauth is sent by the CSG to authorize the quota for the category.

- CSCek43456

  **Description:** When GGSN sends a GGSN call detail record (G-CDR), it includes the QoS profile information element (IE), with one octet added at the end of the field.

  The GGSN receives the QoS Profile IE from the SGSN in the create PDP context request. The length of the field is 12 octets. The QoS Profile encoded by GGSN in the G-CDR has one octet added at the end of the field.

- CSCek49375

  **Description:** A Cisco GGSN running the Release 5.2 image might reload with a "bus error" when creating a PDP context. This reload occurs under the following conditions:

  1. A GPRS tunnel protocol version 0 (GTPv0) service-aware PDP context from SGSN S1 on a transparent mode APN is created.
  2. The same create PDP context request is received from SGSN S2 on the existing PDP.
  3. The PDP is deleted.
  4. Before the path is deleted, another GTPv0 service-aware create PDP context from SGSN S1 is received.

- CSCek50950

  **Description:** A Cisco GGSN running the Release 5.2 image might reload during periods of extreme timing conditions. This reload occurs under the following conditions:

  1. While an update PDP context request is pending on a service-aware PDP context, the GGSN initiates a PDP context deletion.
  2. The GGSN sends the update PDP context response.
  3. Because of path failure, the PDP context is deleted.

- CSCek51987

  **Description:** In a redundant Cisco GGSN configuration, a very large and incorrect value displays on the standby GGSN for prepaid PDP counters. This condition is observed when a prepaid PDP is created on a redundant GGSN setup and send traffic that exceeds quota which was assigned to the PDP.

  If the DCCA server is slow, or is not responding to the reauthorization requests, the PDP is converted to postpaid status. If the prepaid PDP is converted to postpaid status, then the prepaid PDP counter on the standby GGSN shows a very large and incorrect value when displayed using the **show gprs gtp status** command.

- CSCin99848

  **Description:** A Cisco GGSN running the Release 6.0, Cisco IOS Release 12.4(2)XB2 image is not able to lookup the PDP context correctly when the SLB PDP status query contains a NSAPI value between 0 and 4.

- CSCin99850

  **Description:** The Cisco GGSN crashes when the **show gprs gtp pdp tid tid** command is executed during a period of multiple PDP creates and deletes.

- CSCsa53334

  The Intrusion Prevention System (IPS) feature set of Cisco IOS contains several vulnerabilities. These include:

  - Fragmented IP packets may be used to evade signature inspection.
  - IPS signatures utilizing the regular expression feature of the ATOMIC.TCP signature engine may cause a router to crash resulting in a denial of service.

  There are mitigations and workarounds for these vulnerabilities. Cisco has made free software available to address these vulnerabilities for affected customers.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20070213-iosips.shtml.

- CSCsc51539 (duplicate of CSCs02822)

  **Description:** When the GTP IMSI Sticky database feature is enabled on the Cisco IOS SLB, and session redundancy is configured between two GGSNs, after a failover, the newly active GGSN is unable to send a delete notification to the Cisco IOS SLB to delete the previously created sticky entries when the PDP contexts related to those entries are deleted.

- CSCsd76596

  **Description:** With a Cisco GGSN running the Release 5.2 or 6.0 image, all the categories of a service-aware PDP might go into IDLE state when a duplicate create PDP context request is received.

  This condition occurs when the GGSN receives a duplicate create PDP context request for an existing service-aware PDP.

- CSCse05642

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)

  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCse12345

  **Description:** With a Cisco GGSN, when a RAT field is provided in the Create and/or Update PDP Context request, the value encoded in RADIUS Access-Request and Accounting-Request packets has an incorrect length.

  This condition occurs when a RAT field is provided in a Create or Update PDP Context request.

- CSCse50873

  **Description:** QoS displays all zeros for GTPv1 PDPs in the **show gprs gtp pdp-context** output.

- CSCse62599

  **Description:** A Cisco GGSN reloads when rare passwords are used. This reload occurs when the create PDP context request uses the virtual APN feature and the password has the "@password" character.

- CSCse64581

  **Description:** A Cisco GGSN running the release 5.x or 6.0 image reloads when a secondary create PDP context is received with a TFT IE that has the TFT code as "No TFT operation" and the packet has a filter. This condition occurs only when the **debug gprs gtp parsing** command is enabled.

- CSCse66427

  **Description:** In a redundant Cisco GGSN configuration, an incorrect, and very large value, displays for prepaid PDP counters on the standby GGSN. This condition is seen when the following scenario occurs:

  1. A GTPv0 PDP context is created.
  2. When the **show gprs gtp status c**ommand is issued on the standby GGSN, the counter for the prepaid PDP counter displays an incorrect value.
  3. The GTPv0 PDP context is deleted.
  4. The counter on the standby GGSN for the for the prepaid PDP now displays a very large and incorrect value when the show gprs gtp status command is issued.

- CSCse68138

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254

  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned 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.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCse79433

  **Description:** Stale PDP contexts are not deleted on the Cisco GGSN even when the **clear gprs gtp pdp-context** command is used. This condition occurs if an attempt to create a prepaid PDP context is made while the DCCA server is in the peer down state.

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

- CSCsf05276

  **Description:** The output displayed by the **show gprs redundancy** command displays wrong counter values. The “Total number of Messages” value does not match with the sum of the values from the messages.

## Closed Caveat

The following caveat was closed in Cisco IOS Release 12.4(2)XB3.

- CSCsd82253

  **Description:** GGSN GTP session redundancy requires consistent configuration on the Active and Standby IOS instances. An inconsistent IP address pool configuration would cause GGSN to reload unexpectedly.

  **Workaround:** Ensure that the configuration of the Active and Standby GGSN are consistent.

# Caveats—Cisco IOS Release 12.4(2)XB2

The following caveats are open and resolved in Cisco IOS Release 12.4(2)XB2.

## Open Caveats

The following caveat is open in the Cisco IOS Release 12.4(2)XB2, Cisco GGSN Release 6.0 image.

- CSCej21472

  **Description:** In Cisco IOS GGSN Release 6.0, when an extended QoS profile is sent to the GGSN, the debugs do not correctly display the QoS profile. Octets 15 and 16 of the extended QoS IE show incorrect values for the extended maximum and guaranteed bit rates for downlink.

  This condition occurs when an extended QoS IE is sent in a create PDP context request.

  **Workaround:** There is currently no known workaround.

- CSCek37616

  **Description:** An additional attribute, CC-tariff-change-units, is sent in the CCR(Update) message to the Diameter server with value of “units-indeterminate” when a SERVICE-REAUTH message is received from CSG after a Tariff-Time change.

  This condition occurs with the following:

  a. The PDP context is service aware.
  b. A Tariff-Time change event occurs for services associated with the PDP context and a CCR(Update) is sent to the Diameter server.
  c. Quota is allocated to the service by Diameter server in a CCA(Update) message.
  d. Another Service-Reauth is sent by the CSG to authorize the quota for the category.

  **Workaround:** There is currently no known workaround.

- CSCsc12830

  **Description:** A Cisco GGSN configured for service-aware functionality might show a mismatch of the GTP status counters. The “activated pdp” and “activated ms” counters in the GTP status output (the **show gprs gtp status** command) might not correctly reflect the actual number of PDP contexts in the system. At this point it is not confirmed which counter is wrong.

  This condition occurs in a service-aware environment with a large number of prepaid PDP contexts being setup while the Diameter Credit Control Application Server is slow in responding and a lot of Tx timeouts occur.

  **Workaround:** There is currently no known workaround.

- CSCsc51539

  **Description:** When the GTP IMSI Sticky database feature is enabled on the Cisco IOS SLB, and session redundancy is configured between two GGSNs, after a failover, the newly active GGSN is unable to send a delete notification to the Cisco IOS SLB to delete the previously created sticky entries when the PDP contexts related to those entries are deleted.

  **Workaround:** If dispatched mode on the GTP SLB is required, there is currently no known workaround.

- CSCsd82253

  **Description:** GGSN GTP session redundancy requires consistent configuration on the Active and Standby IOS instances. An inconsistent IP address pool configuration would cause GGSN to reload unexpectedly.

  **Workaround:** Ensure that the configuration of the Active and Standby GGSN are consistent.

- CSCse12345

  **Description:** With a Cisco GGSN, when a RAT field is provided in the Create and/or Update PDP Context request, the value encoded in RADIUS Access-Request and Accounting-Request packets has an incorrect length.

  This condition occurs when a RAT field is provided in a Create or Update PDP Context request.

  **Workaround:** There is currently no known workaround.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB2.

- CSCei37916

  **Description:** A Cisco router running Cisco GGSN Release 5.2 displays incorrect behavior when both wait accounting and AAA broadcast accounting are configured for an APN. When the first RADIUS server responds to an Accounting Start, the GGSN establishes the PDP context without waiting for the responses from all the other RADIUS servers. Sometimes under stress conditions, the GGSN might reload.

- CSCei64470

  **Description:** Currently, the Standby GGSN attempts to create CEF adjacency to the SGSN for each of the GTP paths. Creating CEF adjacency if the SGSN and GGSN have not established Level 2 adjacency, requires that Proxy-ARP be configured on the next hop interface. Additionally, two or more nodes might respond to the ARP request, which leads to undesirable routing.

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

  http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

- CSCek28967

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, the create PDP context request is rejected when octet 9 of the QoS IE has a value of less than FE and the extended QoS header (octet 15 and 16) are present.

- CSCek32859

  **Description:** In Cisco IOS Release 12.4(2)XB, the GGSN does not accept the **gprs gtp map signalling tos** command.

- CSCek32989

  **Description:** The Cisco GGSN does not accept a CCA(Update) packet from the Diameter server if there are no Multiple Services Credit Control (MSCC) AVPs in the packet.

  This condition occurs when the following conditions exist for a particular session:

  a. No categories are present for a credit control (CC) session on the GGSN.
  b. An Re-auth Request (RAR) is received for the session.
  c. The CCR(Update) for the session is sent without any MSCC AVPs as there is no quota to report.
  d. The received CCA(Update) does not have any MSCC AVPs because no quota is granted.

  If these conditions occur, the GGSN rejects the CCA(Update) when it should be accepted.

- CSCin98692

  **Description:** Cisco GGSN might reload when the **show aaa attribute protocol radius** command is executed. This occurs only when the command is executed from the command line interface.

- CSCin99623

  **Description:** The connection to a Diameter peer is reset by the Cisco router during periods of low traffic after a Diameter Watchdog Answer (DWA) sent in response to a Diameter Watchdog Request (DWR) has been missed.

  This problem occurs due to a missed DWA message from the DIAMETER server. Typical sequence of events are the following:

  a. The router sends a DWR to the Diameter server.
  b. There is a period of high traffic, during which a lot of messages are received from the server, but a DWA is not received.
  c. The traffic eases up, and the rate at which messages are received slows (the Tw expires after the last message received from the Diameter server).
  d. The connection to the Diameter server is reset.

- CSCsb25337

  Cisco devices running Cisco IOS, which support voice and are not configured for Session Initiated Protocol (SIP) are vulnerable to a crash under yet to be determined conditions, but isolated to traffic destined to User Datagram Protocol (UDP) 5060. SIP is enabled by default on all Advanced images which support voice and do not contain the fix for CSCsb25337. Devices which are properly configured for SIP processing are not vulnerable to this issue. Workarounds exist to mitigate the effects of this problem. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml

- CSCsc09233

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, cGgsnSlbNotif might retain the previous value even if the corresponding configuration is removed using **no** form of the **gprs slb notify** command from the GGSN.

- CSCsc12583

  **Description:** The GGSN might reload under control and data traffic stress conditions. The condition most like to produce this reload is overlapping create PDP and delete PDP context requests for a large number of PDP contexts. One such scenario would be a SGSN path failure and subsequent deletion of a large number of PDP contexts while new create PDP context requests are arriving.

- CSCsc98272

  **Description:** The Cisco GGSN has a high packet drop rate for the 512-byte size packets. This condition occurs when there are 60,000 PDPs spread across 500 VRF-APNs, 120 PDPs per APN, the CPU is approximately 30 percent, the packet rate is approximately 14097 PPS downstream and 3524 PPS upstream, and the GGSN is implemented on the Catalyst 6500 / Cisco 7600 MWAM platform.

- CSCsc98342

  **Description:** In a GTP session redundancy configuration, upon becoming the newly active GGSN, the GGSN reloads and loses all the PDP contexts.

  This condition occurs when the CPU is kept high (approximately 70-80%), with 60,000 PDP contexts spread across 500 VRF-APNs, each APN has 120 PDP contexts, and a switchover from Active GGSN to Standby GGSN is done.

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd58381

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

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

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml

- CSCsd66755

  **Description:** When interim accounting is not configured on the GGSN, the updated values of the SGSN address and negotiated QOS do not appear in the Accounting-Stop message.

  This condition occurs when the following conditions exist:

  a. Interim accounting is not configured under the APN.
  b. A GTPv1 PDP is created.
  c. An Update request is received with a new SGSN Address or negotiated QOS value.
  d. The PDP is deleted.
  e. The corresponding Accounting-Stop still has the SGSN address and negotiated QOS values received in the create PDP context request.

- CSCsd77731

  **Description:** A Cisco GGSN operating in a Diameter Credit Control Application (DCCA) prepaid environment might reload under stress conditions when multiple DCCA servers are supported for server redundancy.

  Specifically, this GGSN exception might occur when the following conditions exist:

  a. Multiple DCCA servers are configured in the same AAA server group.

  b. The Diameter transaction timer and DCCA Tx timer are not configured correctly. (The recommendation is that the Diameter transaction timer be reasonably higher than the Tx timer. The default for the Diameter transaction timer is 30 seconds and the default for the Tx timer is 10 seconds).

  c. The Diameter servers are slow in response.

- CSCsd80775

  **Description:** The Cisco GGSN sends an incorrect Msg-length subfield for PAP Authenticate-Ack frames in the Create PDP Context response. The data field inside the Authenticate-Ack frame contains a 1-byte Msg-length subfield that specifies the length of the Message subfield that follows it.

  The Msg-length subfield contains an arbitrary string of data. The use of this data is implementation-dependent—it might be used to indicate authentication success or failure to a user. If not used, the Msg-length subfield is included, but its value is set to zero. This condition does not have an operational impact on PAP authentication, however, it can cause monitoring issues.

  To resolve this condition, configure the **gprs gtp response-message pco ipcp message length** global configuration command to configure the GGSN to include the Msg-length subfield in PAP Authenticate-Ack frames.

- CSCse04545

  **Description:** In an enhanced service-aware environment, with the Cisco GGSN functioning as a Diameter Credit Control Application (DCCA) client, the GGSN does not set the Diameter watchdog timer (Tx) correctly.

  The GGSN sends a Device-Watchdog-Request (DWR) and starts the Tw when messages from the DCCA server are pending. When the Credit Control Answers (CCAs) are received from the DCCA server before the expiration of the Tw timer, the GGSN should reset the Tw timer, but it doesn't. Instead, after the Tx timer expires, the GGSN marks the Diameter peer as DOWN and fails over to the secondary server.

  The GGSN should reset the Tx timer when it receives any AAA message from the Diameter server (and not necessarily a DWA to the DWR).

# Caveats—Cisco IOS Release 12.4(2)XB1

The following caveats are open, resolved, unreproducible, and closed in Cisco IOS Release 12.4(2)XB1.

## Open Caveats

The following caveat is open in the Cisco IOS Release 12.4(2)XB1, Cisco GGSN Release 6.0 image.

- CSCeg03019

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, when both generic routing encapsulation (GRE) and IP in IP (IPIP) tunnels are configured, and a packet traverses both, Cisco Express Forwarding (CEF) might not work.

  **Workaround:** There is currently no known workaround.

- CSCeh56728

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, if a PSD is overwritten with a new PSD when there are pending CDRs in the queue, new CDRs are not forwarded to the new PSD. If this condition occurs, the charging gateways have to be shut down to force the CDRs to queue up.

  **Workaround:** There is currently no known workaround.

- CSCej21472

  Description: In Cisco IOS GGSN Release 6.0, when an extended QoS profile is sent to the GGSN, the debugs do not correctly display the QoS profile. Octets 15 and 16 of the extended QoS IE show incorrect values for the extended maximum and guaranteed bit rates for downlink.

  This condition occurs when an extended QoS IE is sent in a create PDP context request.

  **Workaround:** There is currently no known workaround.

- CSCin98692

  **Description:** Cisco GGSN might reload when the **show aaa attribute protocol radius** command is executed. This occurs only when the command is executed from the command line interface.

  **Workaround:** There is currently no known workaround.

- CSCsa88617

  **Description:** Under some conditions, packets appear on the network that are not normal GTP packets. These packets appear to originate in the PSD and be addressed to the GGSN.

  **Workaround:** There is currently no known workaround.

- CSCsb54723

  **Description:** cPSDDownNotif might not be sent by the GGSN when the PSD server IP configuration is removed from the GGSN.

  **Workaround:** There is currently no known workaround.

- CSCsb72151

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, during the call detail record (CDR) retrieval, sometimes the PSD does not send an echo-response to the GGSN, which causes the GGSN to mark the PSD link as down.

  **Workaround:** Configure the **gprs charging reconnect** global configuration command to ensure that the GGSN periodically attempts to reconnect to determine when the link is back up.

- CSCsc09233

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, cGgsnSlbNotif might retain the previous value even if the corresponding configuration is removed using **no** form of the **gprs slb notify** command from the GGSN.

  **Workaround:** There is currently no known workaround.

- CSCsc11366

  **Description:** The Cisco GGSN might delay sending charging data records (CDRs) when a node alive message is received from the charging gateway. This condition occurs only when the charging gateway has been marked as “down” in the GGSN and then a node alive is received. Currently there is no known workaround.

  **Workaround:** There is currently no known workaround.

- CSCsc12583

  **Description:** The GGSN might reload under control and data traffic stress conditions. The condition most like to produce this reload is overlapping create PDP and delete PDP context requests for a large number of PDP contexts. One such scenario would be a SGSN path failure and subsequent deletion of a large number of PDP contexts while new create PDP context requests are arriving.

  **Workaround:** There is currently no known workaround.

- CSCsc12830

  **Description:** A Cisco GGSN configured for service-aware functionality might show a mismatch of the GTP status counters. The “activated pdp” and “activated ms” counters in the GTP status output (the **show gprs gtp status** command) might not correctly reflect the actual number of PDP contexts in the system. At this point it is not confirmed which counter is wrong.

  This condition occurs in a service-aware environment with a large number of prepaid PDP contexts being setup while the Diameter Credit Control Application Server is slow in responding and a lot of Tx timeouts occur.

  **Workaround:** There is currently no known workaround.

- CSCsc46179

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, unconfiguring a retrieve-only PSD server causes it to become a read-write PSD server.

  **Workaround:** There is currently no known workaround.

- CSCsc49575

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, cGgsnSANotifCsgRealAddress might be 0.0.0.0 when cGgsnSACsgStateDownNotif or cGgsnSACsgStateUpNotif traps are generated.

  **Workaround:** There is currently no known workaround.

- CSCsc60231

  **Description:** Cisco GGSN R6.0 might cause a traceback while trying to create a PDP context without specifying a bandwidth in the **gprs qos bandwidth-pool** command.

  This condition occurs only when **debug gprs gtp event** is enabled and a bandwidth is not configured for the bandwidth pool.

  **Workaround:** Do not specify the **debug gprs gtp event** command.

- CSCsc98272

  **Description:** The Cisco GGSN has a high packet drop rate for the 512-byte size packets. This condition occurs when there are 60,000 PDPs spread across 500 VRF-APNs, 120 PDPs per APN, the CPU is approximately 30 percent, the packet rate is approximately 14097 PPS downstream and 3524 PPS upstream, and the GGSN is implemented on the Catalyst 6500 / Cisco 7600 MWAM platform.

  **Workaround:** There is currently no known workaround.

- CSCsc51539

  **Description:** When the GTP IMSI Sticky database feature is enabled on the Cisco IOS SLB, and session redundancy is configured between two GGSNs, after a failover, the newly active GGSN is unable to send a delete notification to the Cisco IOS SLB to delete the previously created sticky entries when the PDP contexts related to those entries are deleted.

  **Workaround:** If dispatched mode on the GTP SLB is required, there is currently no known workaround.

- CSCsc94608

  **Description:** In Cisco Mobile Exchange (CMX) environment, the Cisco Content Services Gateway (CSG) is configured to send RADIUS Packet of Disconnect (PoD) packets to the GGSN when a user disconnect request from the quota server is received. The CSG is configured to report 3GPP IMSI (26/10415/1) and NSAPI (26/10415/10) in the RADIUS PoD. With this configuration, when the CSG sends the PoD, the GGSN reports an unsupported attribute and VSA form error and drops the PoD request, but does not delete the PDP context.

  This condition only occurs when the CSG is configured to report 3GPP IMSI and NSAPI in the RADIUS PoD. When sub-attributes are used, the CSG encodes them in a single VSA. If the CSG is configured to send RADIUS Accounting Session Id in the PoD message instead of the IMSI and NSAPI, then the GGSN accepts the message and deletes the PDP context and everything works as designed.

  **Workaround:** Configure the CSG to report RADIUS Accounting Session Id in the PoD message/

- CSCsc98342

  **Description:** In a GTP session redundancy configuration, upon becoming the newly active GGSN, the GGSN reloads and loses all the PDP contexts.

  This condition occurs when the CPU is kept high (approximately 70-80%), with 60,000 PDP contexts spread across 500 VRF-APNs, each APN has 120 PDP contexts, and a switchover from Active GGSN to Standby GGSN is done.

  **Workaround:** There is currently no known workaround.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB1.

- CSCej09790

  **Description:** In the Cisco GGSN, when a service-aware secondary PDP is created, it always has a charging characteristic selection mode value of “subscriptionSpecific.” However, this value is only used when the charging characteristic is assigned by AAA. The secondary PDP needs to reflect the same charging characteristics value that is used by the primary.

- CSCej38935

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, when a path failure occurs on the Cisco GGSN to the SGSN, and there are bursts of create PDP context requests being sent to the GGSN, some PDP contexts might not be recreated on the standby GGSN.

- CSCej48454

  **Description:** The GGSN interface inputq might lose communication when the following condition occurs:

  a. APN redirect all feature is enabled
  b. GGSN receives user payload packet destined for internal loopback address. The packet size is less than 1500.
  c. The packet includes something that cannot be CEF switched.

- CSCej57222

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, with a long duration of GTP path setups and GTP path echo failures, the standby GGSN might have hanging PDP paths even though all paths on the active GGSN are released.

- CSCej79360

  **Description:** The TCP path between a charging gateway and a Cisco GGSN might flap when the following conditions occur:

  a. Redirect all is enable (redirect all IP command).
  b. Many redirect all traffic needs to be redirected (punted) to the process level because there is IP option field in the packet.
  c. The charging path protocol is TCP.

  This condition occurs when the GGSN send 128 charging messages simultaneously, but the TCP send window is only 20K bytes. Therefore, many of the packet are dropped before leaving the GGSN. After the maximum number of retries, and no response, the GGSN will mark the charging gateway as down.

- CSCej85613

  **Description:** A Cisco router running Cisco GGSN software might not CEF-switch packets.

  This condition occasionally occurs when only downstream packets are being sent to the GGSN. GGSN complains about no adjacency being setup and the packets are process switched.

- CSCsa85015

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, a traceback indicating bad refcount occurs on the GGSN at some times. This condition occurs when the redirect all ip feature is enabled (using the **redirect all ip** access point configuration command), or the GTP payload packet is not an IP packet or is an incorrectly formatted IP packet. This condition does not impact service or cause any other side effects.

- CSCsb94067

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, an SNMP query on cgprsAccPtSecNetbiosServer might return a “Packet too big” error.

- CSCsb96863

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, when a CCR(Update) is sent due to a Service-Auth message from the CSG for a category that was previously IDLE, it contains the Reporting-Reason attribute. This attribute should not be present unless usage is being reported in a CCR message.

  This condition is recreated by the following steps:

  a. Create a service-aware PDP.
  b. Create a service (for example, service 1), by sending a service-auth.
  c. Terminate the service by sending service-stop.
  d. Recreate the service by sending a service-auth again.

     In the CCR(U) sent, due to Step 4., we see the reporting-reason attribute extra.

- CSCsc19635

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, a software forced crash might bring down an IOS instance on an MWAM processor after the instance has taken over some HSRP groups.

  This condition occurs when HRSP is configured and the instance takes over some HRSP groups.

- CSCsc20881

  **Description:** The Cisco GGSN advertises the downlink nexthop only if the APN is "service-aware." If the APN is not service-aware, then the downlink_nexthop VSA is not sent in the RADIUS accounting-start messages even if the APN is configured with the **advertise downlink next-hop** *ip* command.

- CSCsc35963

  **Description:** In Cisco IOS Release 12.4(2)XB, for service-aware PDPs, when the threshold is sent by the GGSN in a Quota-Push or Service-Auth Response message to the CSG, the CSG does not honor that request. This condition occurs when the APN is configured for service-aware PDPs.

- CSCsc38829

  **Description:** The Standby GGSN processor in a GTP-SR group might crash (with bus error) during extreme timing situations, such as when a PDP is deleted on the Standby GGSN while PDP context replication on Standby GGSN is occurring.

- CSCsc58186

  **Description:** The Cisco GGSN Call Admission Control (CAC) feature might not work with extended QoS.

- CSCsc60011

  **Description:** In the Cisco GGSN, the Reporting-Reason AVP in the CCR-Final might be incorrect.

  This conditions occurs when the following exists:

  a. The Cause AVP in the received Service-Stop request from the CSG is User-Logged-Out.
  b. The PDP is not terminated.
  c. All the services related to the PDP are terminated.

  When the above occurs, a CCR-Final is sent to the CLCI-S with the Reporting-Reason AVP set to OTHER_QUOTA_TYPE. For the usage type being reported in the Service-Stop request, the Reporting-Reason AVP in the CCR-Final should have a value of FINAL.

- CSCsc65387

  **Description:** When a create PDP context request fails on a GGSN because the CAC policy resource limit has been reached, and Cisco IOS SLB fails on its maximum reassign attempts to other GGSNs without the expected create PDP context response failure with cause 199 (NO RESOURCE) being sent to the SGSN because of an incorrect sequence number in the CAC reassign notification message from the GGSN to the Cisco IOS SLB.

  This condition occurs under severe conditions when all the GGSNs tried by the Cisco IOS SLB have run out of resources for the APN as defined by the CAC policy.

- CSCsc70585

  **Description:** The Cisco CSG queues up the GTP' messages and retransmits. As long as there are messages received from the quota server, CSG does not mark the quota server failed. Once all the 50K users are active and no new quota server traffic is present. The retransmits from the queue are not responded to. GGSN drops these packets because it has already responded to them. CSG reaches its retransmit interval/max and marks the GGSN as failed. If GGSN acknowledges the retransmitted packet, the Cisco CSG will remove the GTP' message from the queue and not mark the GGSN as failed.

- CSCsc84735

  **Description:** Cisco GGSN R5.2 does not delete the PDP context after it receives a result code of 5002 in the CCA final message.

  This condition occurs when the Diameter server sends a CCA final with an error code of 5002

- CSCsc86028

  **Description:** A Cisco GGSN R6.0 image does not display conditional MSISDN debugs after the PDP context is deleted and created again. The debugs are displayed only for the first time.

### Unreproducible Caveat

The Cisco GGSN caveat listed in this section has not been reproduced during testing. In the unlikely event you experience the problem described in this section, contact Cisco customer service.

- CSCsc04803

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, you might not be able to set or get cGgsnSAServiceAware if the **gprs service-aware** global configuration command is not configured.

## Caveats—Cisco IOS Release 12.4(2)XB

The following caveats are open, resolved, and closed in Cisco IOS Release 12.4(2)XB.

### Open Caveats

The following caveat is open in the Cisco IOS Release 12.4(2)XB, Cisco GGSN Release 6.0 image.

- CSCeg03019

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, when both generic routing encapsulation (GRE) and IP in IP (IPIP) tunnels are configured, and a packet traverses both, Cisco Express Forwarding (CEF) might not work.

  **Workaround:** There is currently no known workaround.

- CSCeh56728

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, if a PSD is overwritten with a new PSD when there are pending CDRs in the queue, new CDRs are not forwarded to the new PSD. If this condition occurs, the charging gateways have to be shut down to force the CDRs to queue up.

  **Workaround:** There is currently no known workaround.

- CSCej38935

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, when a path failure occurs on the Cisco GGSN to the SGSN, and there are bursts of create PDP context requests being sent to the GGSN, some PDP contexts might not be recreated on the standby GGSN.

  **Workaround:** Disable Echo Timing on the GTP path on the GGSN.

- CSCej57222

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, with a long duration of GTP path setups and GTP path echo failures, the standby GGSN might have hanging PDP paths even though all paths on the active GGSN are released.

  **Workaround:** There is currently no known workaround.

- CSCsa85015

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, a traceback indicating bad refcount occurs on the GGSN at some times. This condition occurs when the redirect all ip feature is enabled (using the **redirect all ip** access point configuration command), or the GTP payload packet is not an IP packet or is an incorrectly formatted IP packet. This condition does not impact service or cause any other side effects.

  **Workaround:** Unconfigure the **redirect all ip** command, however, since this condition does not impact services, a workaround might not be necessary.

- CSCsa88617

  **Description:** Under some conditions, packets appear on the network that are not normal GTP packets. These packets appear to originate in the PSD and be addressed to the GGSN.

  **Workaround:** There is currently no known workaround.

- CSCsb54723

  **Description:** cPSDDownNotif might not be sent by the GGSN when the PSD server IP configuration is removed from the GGSN.

  **Workaround:** There is currently no known workaround.

- CSCsb72151

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, during the CDR retrieval, sometimes the PSD does not send an echo-response to the GGSN, which causes the GGSN to mark the PSD link as down.

  **Workaround:** Configure the **gprs charging reconnect** global configuration command to ensure that the GGSN periodically attempts to reconnect to determine when the link is back up.

- CSCsb94067

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, an SNMP query on cgprsAccPtSecNetbiosServer might return a “Packet too big” error.

  **Workaround:** There is currently no known workaround.

- CSCsb96863

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, when a CCR(Update) is sent due to a Service-Auth message from the CSG for a category that was previously IDLE, it contains the Reporting-Reason attribute. This attribute should not be present unless usage is being reported in a CCR message.

  This condition is recreated by the following steps:

  a. Create a service-aware PDP.

  b. Create a service (for example, service 1), by sending a service-auth.

  c. Terminate the service by sending service-stop.

  d. Recreate the service by sending a service-auth again.

     In the CCR(U) sent, due to Step 4., we see the reporting-reason attribute extra.

  **Workaround:** There is currently no known workaround.

- CSCsc04803

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, you might not be able to set or get cGgsnSAServiceAware if the **gprs service-aware** global configuration command is not configured.

  **Workaround:** Use **gprs service-aware** and **no gprs service-aware** global configuration commands.

- CSCsc09233

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, cGgsnSlbNotif might retain the previous value even if the corresponding configuration is removed using **no** form of the **gprs slb notify** command from the GGSN.

  **Workaround:** There is currently no known workaround.

- CSCsc19635

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, a software forced crash might bring down an IOS instance on an MWAM processor after the instance has taken over some HSRP groups.

  This condition occurs when HRSP is configured and the instance takes over some HRSP groups.

  **Workaround:** Ensure that the charging header is configured properly. For example, if the charging gateway is using a short header, then the GGSN should be configured to use the short header using the **gprs charging header short** global configuration command.

- CSCsc35963

  **Description:** In Cisco IOS Release 12.4(2)XB, for service-aware PDPs, when the threshold is sent by the GGSN in a Quota-Push or Service-Auth Response message to the CSG, the CSG does not honor that request. This condition occurs when the APN is configured for service-aware PDPs.

  **Workaround:** There is currently no known workaround.

- CSCsc38829

  **Description:** The Standby GGSN processor in a GTP-SR group might crash (with bus error) during extreme timing situations, such as when a PDP is deleted on the Standby GGSN while PDP context replication on Standby GGSN is occurring.

  **Workaround:** There is currently no known workaround.

- CSCsc46179

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, unconfiguring a retrieve-only PSD server causes it to become a read-write PSD server.

  **Workaround:** There is currently no known workaround.

- CSCsc49575

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, cGgsnSANotifCsgRealAddress might be 0.0.0.0 when cGgsnSACsgStateDownNotif or cGgsnSACsgStateUpNotif traps are generated.

  **Workaround:** There is currently no known workaround.

## Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.4(2)XB.

- CSCsb84438

  **Description:** A Cisco router running GGSN software might reload if the following condition persists for an extended period of time:

  a. The DHCP server is very slow.
  b. The User session activation is high.
  c. The DHCP lease is very short.

- CSCeh69873

  **Description:** When a GGSN receives a PDP context with non-real time traffic classes and an SSD value is not 1 (i.e. speech), the PDP context is rejected.

- CSCsb43916

  **Description:** During the failover transition of redundant GGSNs, the active GGSN sends a redundancy status of ACTIVE/ACTIVE (SNMP trap integer 14) for both peers to the SNMP host when it should send (Active/Disabled) or (Active/Standby).

- CSCsc05462

  **Description:** In Cisco IOS Release 12.3(14)YQ3 (Cisco GGSN Release 5.2), a PLMN and QoS change at the same time causes a duplicated volume report. The same byte counts are reported in successive containers, one added for record closure due to PLMN change, and the other added due to QoS Change. No charging profile is configured under the APN because it is not service-aware (GGSN functionality testing). SGSN didn't send any Charging-characteristics value.

- CSCej48899

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, there are several record closure containers within one CDR when an update request occurs more than once with the RAT and newly supported IEs being changed. The trigger does not reset the values, so the values are repeated.

- CSCsc25722

  **Description:** In a Cisco GGSN running Cisco IOS Software Release 12.4(2)XB, an Authentication Fail trap is not sent if there is an incorrect username or password.

- CSCsc31776

  **Description:** In Cisco IOS GGSN Release 5.0 and 6.0, the router reloads when 3000 create PDP context requests are sent and the following configurations exist:

  a. The **debug gprs gtp message** command is configured.
  b. An external DHCP IP address assignment is configured.
  c. VRF is configured on the APN but not on the DHCP server.

- CSCej72003

  **Description:** With an SGSN change, RAT change, and Qos change, the Data volume sent is negative with the charging profile being used under the APN and the profile does not have reset for triggers.

- CSCej48745

  **Description:** The Data volume content is wrong when a RAT change causes a CDR to close.

### Closed Caveat

The following caveat is closed.

- CSCsc06275

  **Description:** In a Cisco GGSN running Cisco IOS Release 12.4(2)XB, the Cisco IOS SLB operation mode for GGSN-SLB messaging might not be configurable using the **no gprs slb mode** global configuration command (the mode option might not be available).

# Cisco MWAM Caveats, with Cisco IOS Release 12.4 XB

This section lists the Cisco MWAM caveats that are open and resolved with the Cisco IOS Release 12.4 XB releases.

## Caveats—with Cisco IOS Release 12.4(2)XB11

This section lists the Cisco MWAM caveats that are open and closed with Cisco IOS Release 12.4(2)X11.

### Open Caveat

There are no known caveats open in the Cisco IOS Release 12.4(2)XB7 Cisco GGSN Release 6.0 image.

### Closed Caveats

The following caveat has been closed in Cisco IOS Release 12.4(2)XB11.

- CSCek31236

  **Description:** The system restart time is wrong in **show version** command output. It increases over time.

# Caveats—with Cisco IOS Release 12.4(2)XB10

This section lists the Cisco MWAM caveats that are open and resolved with Cisco IOS Release 12.4(2)X10.

## Open Caveat

The following Cisco MWAM caveat is open with Cisco IOS Release 12.4(2)XB10.

- CSCek31236

  **Description:** The system restart time is wrong in **show version** command output. It increases over time.

  **Workaround:** There is currently no known workaround.

## Resolved Caveats

The following Cisco MWAM caveats have been resolved for Cisco IOS Release 12.4(2)XB10.

- 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(2)XB8

This section lists the Cisco MWAM caveats that are open and resolved with Cisco  Release 12.4(2)XB8.

## Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.4(2)XB8.

- CSCef74977

  **Description:** If a Supervisor switchover occurs while a reload all is in progress on an MWAM, the some CPUs might be left in an inactive state. If this occurs, the following message might display:

  ```
  <MWAM: No response from IOS complex n, resetting complex.>
  ```

  where *n* is the complete number 0, 1, or 2.

  This condition occurs in rare cases when a Supervisor switchover is triggered immediately after the **reload all** command is issued on the MWAM to reload all the MWAM processors.

  **Workaround:** There is currently no known workaround.

- CSCef76954

  **Description:** The session from the Supervisor 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.

- CSCeg13327

  **Description:** Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

  This condition occurs when a GRE tunnel is established between two MWAM processors of the same sibyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

  **Workaround:** There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCsg04707

  **Description:** The following error message is seen when the configuration is saved:

  ```
  %SCHED-3-SEMLOCKED: Virtual Exec attempted to lock a semaphore, already locked by
  itself -Traceback= 0x2067F130 0x20798C90 0x2068BE74 0x2068C878 0x208182B8 0x20813554
  0x2081358C 0x2080CCE8 0x208203A4 0x208165EC 0x20821050 0x206BC748 0x206D1728
  0x206D164C 0x2075D408 0x2075D488
  ```

  This condition occurs on the MWAM when running the GGSN, Cisco IOS Release 12.4(2)XB2 or later image, but it is not platform specific. This condition occurs when the **privilege exec all level 5 copy** command is configured.

  **Workaround:** Ensure that the **privilege exec all level 5 copy** command is not configured.

- CSCsb59293

  **Descriptions:** Configurations are written to MWAM processor NVRAM even when there is an error writing to the Supervisor during a "write mem." This causes the **show startup-config** command display to miss its synchronization with the configuration on the Supervisor, and therefore, display a configuration different from the one with which MWAM will boot the next time.

  This condition occurs when the MWAM configuration mode is Supervisor and there is an error writing to the Supervisor from the MWAM (for example, when there is an incorrect rcmd configuration on the Supervisor).

  **Workaround:** When the **write mem** command returns a response that the configuration could not be written to the Supervisor, troubleshoot the cause and repeat the command.

- CSCsb62456

  **Description:** MWAM processor 3 is unable to ping outside interfaces after an image upgrade. This condition can be reproduced by switching to MP mode and from the AP.

  **Workaround:** Reset the MWAM by issuing the **hw-module module** *slot_number* **reset** command.

## Resolved Caveat

There are no new Cisco MWAM caveats resolved for Cisco IOS Release 12.4(2)XB8.

# Caveats—with Cisco IOS Release 12.4(2)XB7

This section lists the Cisco MWAM caveats that are open and resolved with Cisco IOS Release 12.4(2)XB7.

## Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.4(2)XB7.

- CSCef74977

  **Description:** If a Supervisor switchover occurs while a reload all is in progress on an MWAM, the some CPUs might be left in an inactive state. If this occurs, the following message might display:

  ```
  <MWAM: No response from IOS complex n, resetting complex.>
  ```

  where *n* is the complete number 0, 1, or 2.

  This condition occurs in rare cases when a Supervisor switchover is triggered immediately after the **reload all** command is issued on the MWAM to reload all the MWAM processors.

  **Workaround:** There is currently no known workaround.

- CSCef76954

  **Description:** The session from the Supervisor 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.

- CSCeg13327

  **Description:** Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

  This condition occurs when a GRE tunnel is established between two MWAM processors of the same sibyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

  **Workaround:** There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCsg04707

  **Description:** The following error message is seen when the configuration is saved:

  ```
  %SCHED-3-SEMLOCKED: Virtual Exec attempted to lock a semaphore, already locked by
  itself -Traceback= 0x2067F130 0x20798C90 0x2068BE74 0x2068C878 0x208182B8 0x20813554
  0x2081358C 0x2080CCE8 0x208203A4 0x208165EC 0x20821050 0x206BC748 0x206D1728
  0x206D164C 0x2075D408 0x2075D488
  ```

  This condition occurs on the MWAM when running the GGSN, Cisco IOS Release 12.4(2)XB2 or later image, but it is not platform specific. This condition occurs when the **privilege exec all level 5 copy** command is configured.

  **Workaround:** Ensure that the **privilege exec all level 5 copy** command is not configured.

- CSCsb59293

  **Descriptions:** Configurations are written to MWAM processor NVRAM even when there is an error writing to the Supervisor during a “write mem.” This causes the **show startup-config** command display to miss its synchronization with the configuration on the Supervisor, and therefore, display a configuration different from the one with which MWAM will boot the next time.

  This condition occurs when the MWAM configuration mode is Supervisor and there is an error writing to the Supervisor from the MWAM (for example, when there is an incorrect rcmd configuration on the Supervisor).

  **Workaround:** When the **write mem** command returns a response that the configuration could not be written to the Supervisor, troubleshoot the cause and repeat the command.

- CSCsb62456

  **Description:** MWAM processor 3 is unable to ping outside interfaces after an image upgrade. This condition can be reproduced by switching to MP mode and from the AP.

  **Workaround:** Reset the MWAM by issuing the **hw-module module** *slot_number* **reset** command.

## Resolved Caveat

There are no new Cisco MWAM caveats resolved for Cisco IOS Release 12.4(2)XB7.

# Caveats—with Cisco IOS Release 12.4(2)XB6

The following MWAM caveats are open and resolved with Cisco IOS Release 12.4(2)XB6.

## Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.4(2)XB6.

- CSCef74977

  **Description:** If a Supervisor switchover occurs while a reload all is in progress on an MWAM, the some CPUs might be left in an inactive state. If this occurs, the following message might display:

  ```
  <MWAM: No response from IOS complex n, resetting complex.>
  ```

  where *n* is the complete number 0, 1, or 2.

  This condition occurs in rare cases when a Supervisor switchover is triggered immediately after the **reload all** command is issued on the MWAM to reload all the MWAM processors.

  **Workaround:** There is currently no known workaround.

- CSCef76954

  **Description:** The session from the Supervisor 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.

- CSCeg13327

  **Description:** Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

  This condition occurs when a GRE tunnel is established between two MWAM processors of the same sibyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

  **Workaround:** There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCsg04707

  **Description:** The following error message is seen when the configuration is saved:

  ```
  %SCHED-3-SEMLOCKED: Virtual Exec attempted to lock a semaphore, already locked by
  itself -Traceback= 0x2067F130 0x20798C90 0x2068BE74 0x2068C878 0x208182B8 0x20813554
  0x2081358C 0x2080CCE8 0x208203A4 0x208165EC 0x20821050 0x206BC748 0x206D1728
  0x206D164C 0x2075D408 0x2075D488
  ```

  This condition occurs on the MWAM when running the GGSN, Cisco IOS Release 12.4(2)XB2 or later image, but it is not platform specific. This condition occurs when the **privilege exec all level 5 copy** command is configured.

  **Workaround:** Ensure that the **privilege exec all level 5 copy** command is not configured.

- CSCsb59293

  **Descriptions:** Configurations are written to MWAM processor NVRAM even when there is an error writing to the Supervisor during a "write mem." This causes the **show startup-config** command display to miss its synchronization with the configuration on the Supervisor, and therefore, display a configuration different from the one with which MWAM will boot the next time.

  This condition occurs when the MWAM configuration mode is Supervisor and there is an error writing to the Supervisor from the MWAM (for example, when there is an incorrect rcmd configuration on the Supervisor).

  **Workaround:** When the **write mem** command returns a response that the configuration could not be written to the Supervisor, troubleshoot the cause and repeat the command.

- CSCsb62456

  **Description:** MWAM processor 3 is unable to ping outside interfaces after an image upgrade. This condition can be reproduced by switching to MP mode and from the AP.

  **Workaround:** Reset the MWAM by issuing the **hw-module module** *slot_number* **reset** command.

## Resolved Caveat

The following Cisco MWAM caveat has been resolved for Cisco IOS Release 12.4(2)XB6.

- CSCsf31329

  **Description:** A low IO memory condition and a TCP session to the router requiring a packet of more than 600 bytes might trigger a crash.

# Caveats—with Cisco IOS Release 12.4(2)XB5

The following MWAM caveats are open and resolved with Cisco IOS Release 12.4(2)XB5.

## Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.4(2)XB5.

- CSCef74977

  **Description:** If a Supervisor switchover occurs while a reload all is in progress on an MWAM, the some CPUs might be left in an inactive state. If this occurs, the following message might display:

  ```
  <MWAM: No response from IOS complex n, resetting complex.>
  ```

  where *n* is the complete number 0, 1, or 2.

  This condition occurs in rare cases when a Supervisor switchover is triggered immediately after the **reload all** command is issued on the MWAM to reload all the MWAM processors.

  **Workaround:** There is currently no known workaround.

- CSCef76954

  **Description:** The session from the Supervisor 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.

- CSCeg13327

  **Description:** Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

  This condition occurs when a GRE tunnel is established between two MWAM processors of the same sibyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

  **Workaround:** There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCsg04707

  **Description:** The following error message is seen when the configuration is saved:

  ```
  %SCHED-3-SEMLOCKED: Virtual Exec attempted to lock a semaphore, already locked by
  itself -Traceback= 0x2067F130 0x20798C90 0x2068BE74 0x2068C878 0x208182B8 0x20813554
  0x2081358C 0x2080CCE8 0x208203A4 0x208165EC 0x20821050 0x206BC748 0x206D1728
  0x206D164C 0x2075D408 0x2075D488
  ```

  This condition occurs on the MWAM when running the GGSN, Cisco IOS Release 12.4(2)XB2 or later image, but it is not platform specific. This condition occurs when the **privilege exec all level 5 copy** command is configured.

  **Workaround:** Ensure that the **privilege exec all level 5 copy** command is not configured.

- CSCsb59293

  **Descriptions:** Configurations are written to MWAM processor NVRAM even when there is an error writing to the Supervisor during a "write mem." This causes the **show startup-config** command display to miss its synchronization with the configuration on the Supervisor, and therefore, display a configuration different from the one with which MWAM will boot the next time.

  This condition occurs when the MWAM configuration mode is Supervisor and there is an error writing to the Supervisor from the MWAM (for example, when there is an incorrect rcmd configuration on the Supervisor).

  **Workaround:** When the **write mem** command returns a response that the configuration could not be written to the Supervisor, troubleshoot the cause and repeat the command.

- CSCsb62456

  **Description:** MWAM processor 3 is unable to ping outside interfaces after an image upgrade. This condition can be reproduced by switching to MP mode and from the AP.

  **Workaround:** Reset the MWAM by issuing the **hw-module module** *slot_number* **reset** command.

## Resolved Caveats

There are no new Cisco MWAM caveats resolved for Cisco IOS Release 12.4(2)XB5.

# Caveats—with Cisco IOS Release 12.4(2)XB4

The following MWAM caveats are open and resolved with Cisco IOS Release 12.4(2)XB4.

## Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.4(2)XB4.

- CSCef74977

  **Description:** If a Supervisor switchover occurs while a reload all is in progress on an MWAM, the some CPUs might be left in an inactive state. If this occurs, the following message might display:

  ```
  <MWAM: No response from IOS complex n, resetting complex.>
  ```

  where *n* is the complete number 0, 1, or 2.

  This condition occurs in rare cases when a Supervisor switchover is triggered immediately after the **reload all** command is issued on the MWAM to reload all the MWAM processors.

  **Workaround:** There is currently no known workaround.

- CSCef76954

  **Description:** The session from the Supervisor 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.

- CSCeg13327

  **Description:** Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

  This condition occurs when a GRE tunnel is established between two MWAM processors of the same sibyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

  **Workaround:** There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCsg04707

  **Description:** The following error message is seen when the configuration is saved:

  ```
  %SCHED-3-SEMLOCKED: Virtual Exec attempted to lock a semaphore, already locked by
  itself -Traceback= 0x2067F130 0x20798C90 0x2068BE74 0x2068C878 0x208182B8 0x20813554
  0x2081358C 0x2080CCE8 0x208203A4 0x208165EC 0x20821050 0x206BC748 0x206D1728
  0x206D164C 0x2075D408 0x2075D488
  ```

  This condition occurs on the MWAM when running the GGSN, Cisco IOS Release 12.4(2)XB2 or later image, but it is not platform specific. This condition occurs when the **privilege exec all level 5 copy** command is configured.

  **Workaround:** Ensure that the **privilege exec all level 5 copy** command is not configured.

- CSCsb59293

  **Descriptions:** Configurations are written to MWAM processor NVRAM even when there is an error writing to the Supervisor during a "write mem." This causes the **show startup-config** command display to miss its synchronization with the configuration on the Supervisor, and therefore, display a configuration different from the one with which MWAM will boot the next time.

  This condition occurs when the MWAM configuration mode is Supervisor and there is an error writing to the Supervisor from the MWAM (for example, when there is an incorrect rcmd configuration on the Supervisor).

  **Workaround:** When the **write mem** command returns a response that the configuration could not be written to the Supervisor, troubleshoot the cause and repeat the command.

- CSCsb62456

  **Description:** MWAM processor 3 is unable to ping outside interfaces after an image upgrade. This condition can be reproduced by switching to MP mode and from the AP.

  **Workaround:** Reset the MWAM by issuing the **hw-module module** *slot_number* **reset** command.

## Resolved Caveats

There are no new Cisco MWAM caveats resolved for Cisco IOS Release 12.4(2)XB4.

# Caveats—with Cisco IOS Release 12.4(2)XB3

The following MWAM caveats are open and resolved with Cisco IOS Release 12.4(2)XB3.

## Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.4(2)XB3.

- CSCef74977

  **Description:** If a Supervisor switchover occurs while a reload all is in progress on an MWAM, the some CPUs might be left in an inactive state. If this occurs, the following message might display:

  `<MWAM: No response from IOS complex n, resetting complex.>`

  where *n* is the complete number 0, 1, or 2.

  This condition occurs in rare cases when a Supervisor switchover is triggered immediately after the **reload all** command is issued on the MWAM to reload all the MWAM processors.

  **Workaround:** There is currently no known workaround.

- CSCef76954

  **Description:** The session from the Supervisor 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.

- CSCeg13327

  **Description:** Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

  This condition occurs when a GRE tunnel is established between two MWAM processors of the same sibyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

  **Workaround:** There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCsb59293

  **Descriptions:** Configurations are written to MWAM processor NVRAM even when there is an error writing to the Supervisor during a "write mem." This causes the **show startup-config** command display to miss its synchronization with the configuration on the Supervisor, and therefore, display a configuration different from the one with which MWAM will boot the next time.

  This condition occurs when the MWAM configuration mode is Supervisor and there is an error writing to the Supervisor from the MWAM (for example, when there is an incorrect rcmd configuration on the Supervisor).

  **Workaround:** When the **write mem** command returns a response that the configuration could not be written to the Supervisor, troubleshoot the cause and repeat the command.

- CSCsb62456

  **Description:** MWAM processor 3 is unable to ping outside interfaces after an image upgrade. This condition can be reproduced by switching to MP mode and from the AP.

  **Workaround:** Reset the MWAM by issuing the **hw-module module** *slot_number* **reset** command.

## Resolved Caveats

The following Cisco MWAM caveat has been resolved for Cisco IOS Release 12.4(2)XB3.

- CSCek53232

  **Description:** The MWAM processor crashes when booting up. This crash occur during periods of high CPU due to a large amounts of information printed to the processor (for example, when too much of the configuration is unsupported, or if traffic is being sent when the processor is booting). Workaround: Avoid the possibility of high CPU situation when booting up.

# Caveats—with Cisco IOS Release 12.4(2)XB2

The following MWAM caveats are open and resolved with Cisco IOS Release 12.4(2)XB2.

## Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.4(2)XB2.

- CSCef74977

  **Description:** If a Supervisor switchover occurs while a reload all is in progress on an MWAM, the some CPUs might be left in an inactive state. If this occurs, the following message might display:

  `<MWAM: No response from IOS complex n, resetting complex.>`

  where *n* is the complete number 0, 1, or 2.

  This condition occurs in rare cases when a Supervisor switchover is triggered immediately after the **reload all** command is issued on the MWAM to reload all the MWAM processors.

  **Workaround:** There is currently no known workaround.

- CSCef76954

  **Description:** The session from the Supervisor 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.

- CSCeg13327

  **Description:** Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

  This condition occurs when a GRE tunnel is established between two MWAM processors of the same sibyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

  **Workaround:** There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCej07438

  **Description:** Memory corruption occurs on the MWAM, which might result in crashes or unpredictable behavior. This condition occurs when a timezone name is set on the Supervisor that is longer than three characters (using the **clock timezone** configuration command).

  Note that there are certain conditions possible where this condition might not have an adverse effect if the name length is 4 to 7 characters. However, memory corruption always occurs if the length of the name is more than 7 characters. Configuring the timezone on an MWAM does not trigger this bug.

  **Workaround:** Configure a timezone name on the Supervisor that does not exceed three characters.

- CSCsa48606

  **Description:** The **execute-on** *slot-num* command does not retrieve complete output for the show tech-support on processor 1.

  **Workaround:** There is currently no known workaround.

- CSCsb59293

  **Descriptions:** Configurations are written to MWAM processor NVRAM even when there is an error writing to the Supervisor during a "write mem." This causes the **show startup-config** command display to miss its synchronization with the configuration on the Supervisor, and therefore, display a configuration different from the one with which MWAM will boot the next time.

  This condition occurs when the MWAM configuration mode is Supervisor and there is an error writing to the Supervisor from the MWAM (for example, when there is an incorrect rcmd configuration on the Supervisor).

  **Workaround:** When the **write mem** command returns a response that the configuration could not be written to the Supervisor, troubleshoot the cause and repeat the command.

- CSCsb62456

  **Description:** MWAM processor 3 is unable to ping outside interfaces after an image upgrade. This condition can be reproduced by switching to MP mode and from the AP.

  **Workaround:** Reset the MWAM by issuing the **hw-module module** *slot_number* **reset** command.

- CSCsc44745

  **Description:** In 512- and 1518-packet sizes, packet drops occur at 479-Mbps on one of the MWAM processors. This condition occurs when multiple processors are used.

  **Workaround:** There is currently no known workaround.

- CSCsc73200

  **Description:** A Cisco MWAM might be shutdown for unknown reasons. This condition occurs on a Catalyst 6000 switch with a Supervisor2 running Cisco IOS software version 12.2(17d)SXB5 and the MWAM is running c6svc-5mwam-g4js-bf21_20.123-5a.B4.

  When this condition occurs, the following messages are logged in the MWAM PC complex log:

  ```
  mwam-8 scpd: SCP Registration REQ from 0x8/0.
  mwam-8 scpd: SCP PC Reset.
  mwam-8 scpd: SCP Registration REQ from 0x18/0.
  mwam-8 scpd: SCP PC Shutdown.
  mwam-8 scpd: do_shutdown(): send response.
  mwam-8 scpd: scpd: calling /sbin/shutdown!
  ```

  **Workaround:** There is currently no known workaround.

### Resolved Caveats

There are no new Cisco MWAM caveats resolved for Cisco IOS Release 12.4(2)XB2.

## Caveats—with Cisco IOS Release 12.4(2)XB1

The following MWAM caveats are open and resolved with Cisco IOS Release 12.4(2)XB1.

## Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.4(2)XB1.

- CSCef74977

  **Description:** If a Supervisor switchover occurs while a reload all is in progress on an MWAM, the some CPUs might be left in an inactive state. If this occurs, the following message might display:

  ```
  <MWAM: No response from IOS complex n, resetting complex.>
  ```

  where *n* is the complete number 0, 1, or 2.

  This condition occurs in rare cases when a Supervisor switchover is triggered immediately after the **reload all** command is issued on the MWAM to reload all the MWAM processors.

  **Workaround:** There is currently no known workaround.

- CSCef76954

  **Description:** The session from the Supervisor 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.

- CSCeg13327

  **Description:** Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

  This condition occurs when a GRE tunnel is established between two MWAM processors of the same sibyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

  **Workaround:** There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCej07438

  **Description:** Memory corruption occurs on the MWAM, which might result in crashes or unpredictable behavior. This condition occurs when a timezone name is set on the Supervisor that is longer than three characters (using the **clock timezone** configuration command).

  Note that there are certain conditions possible where this condition might not have an adverse effect if the name length is 4 to 7 characters. However, memory corruption always occurs if the length of the name is more than 7 characters. Configuring the timezone on an MWAM does not trigger this bug.

  **Workaround:** Configure a timezone name on the Supervisor that does not exceed three characters.

- CSCsb59293

  **Description:** Configurations are written to the MWAM processor NVRAM when bootflash access is disabled. This condition occurs when the MWAM configuration mode is Supervisor and the MWAM bootflash access is disabled on the Supervisor.

  **Workaround:** There is currently no known workaround.

- CSCsb62456

  **Description:** MWAM processor 3 is unable to ping outside interfaces after an image upgrade. This condition can be reproduced by switching to MP mode and from the AP.

  **Workaround:** Reset the MWAM by issuing the **hw-module module** *slot_number* **reset** command.

- CSCsc44745

  **Description:** In 512- and 1518-packet sizes, packet drops occur at 479-Mbps on one of the MWAM processors. This condition occurs when multiple processors are used.

  Workaround:

  **Workaround:** There is currently no known workaround.

- CSCsc73200

  **Description:** A Cisco MWAM might be shutdown for unknown reasons. This condition occurs on a Catalyst 6000 switch with a Supervisor2 running Cisco IOS software version 12.2(17d)SXB5 and the MWAM is running c6svc-5mwam-g4js-bf21_20.123-5a.B4.

  When this condition occurs, the following messages are logged in the MWAM PC complex log:

  ```
  mwam-8 scpd: SCP Registration REQ from 0x8/0.
  mwam-8 scpd: SCP PC Reset.
  mwam-8 scpd: SCP Registration REQ from 0x18/0.
  mwam-8 scpd: SCP PC Shutdown.
  mwam-8 scpd: do_shutdown(): send response.
  mwam-8 scpd: scpd: calling /sbin/shutdown!
  ```

  **Workaround:** There is currently no known workaround.

- CSCsc81737

  **Description:** MWAM processor 6 takes more time to come up if bootmode was set from Supervisor mode. If the bootmode is set locally, this condition does not occur.

  **Workaround:** Do not change the configuration mode from the PC complex. Instead, change the configuration mode from the processor using the **mwam config-mode** command.

## Resolved Caveats

There are no new Cisco MWAM caveats resolved for Cisco IOS Release 12.4(2)XB1.

# Caveats—with Cisco IOS Release 12.4(2)XB

The following MWAM caveats are open and resolved with Cisco IOS Release 12.4(2)XB.

## Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.4(2)XB.

- CSCeg13327

  **Description:** Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

  This condition occurs when a GRE tunnel is established between two MWAM processors of the same sibyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

  **Workaround:** There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCej07438

  **Description:** Memory corruption occurs on the MWAM, which might result in crashes or unpredictable behavior. This condition occurs when a timezone name is set on the Supervisor that is longer than three characters (using the **clock timezone** configuration command).

  Note that there are certain conditions possible where this condition might not have an adverse effect if the name length is 4 to 7 characters. However, memory corruption always occurs if the length of the name is more than 7 characters. Configuring the timezone on an MWAM does not trigger this bug.

  **Workaround:** Configure a timezone name on the Supervisor that does not exceed three characters.

- CSCsa50215

  **Description:** Unable to access MWAM processor via session or telnet command for 10 minutes after the processor has been reloaded.

  **Workaround:** Configure the **ip rcmd rcp-enabled** command on the supervisor module.

## Resolved Caveats

The following Cisco MWAM caveats have been resolved for Cisco IOS Release 12.4(2)XB.

- CSCin89403

  **Description:** An MWAM processor does not see the other MWAM processors of a different complex as CDP neighbors. This condition occurs in the Sup22. Each MWAM processor sees just the Supervisor and the MWAM processor of the same complex as CDP neighbors.

- CSCsa48606

  **Description:** The **execute-on** *slot-num* command does not retrieve complete output for the show tech-support on processor 1.

# 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 65
- Platform-Specific Documents, page 66
- Cisco IOS Software Documentation Set, page 66


## 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_roadmap09186a00801ebed9.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 6.0 Configuration Guide and Command Reference and Associated Release Notes for Cisco IOS Release 12.4(2)XB.

  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.



)*Release Notes for Cisco GGSN Release 6.0 on the Cisco MWAM, Cisco IOS Release 12.4 XB*