Release Notes for Cisco GGSN Release 6.0 on the Cisco MWAM, Cisco IOS Software Release 12.4(2)XB6

September 23, 2009

Cisco IOS Release 12.4(2)XB6

These release notes for the Cisco GGSN Release 6.0 on the Cisco Multi-processor WAN Application Module (MWAM) describe the enhancements provided in Cisco IOS Release 12.4(2)XB6. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4(2)XB6, see the "Cisco GGSN Caveats, Cisco IOS Release 12.4(2)XB6" section on page 10 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.

Contents

These release notes describe the following topics:

- Introduction to Cisco GGSN on the Cisco MWAM, page 2
- System Requirements, page 3
- Related Documentation, page 16
- Limitations, Restrictions, and Important Notes, page 5
- New and Changed Information, page 7
- Cisco GGSN Caveats, Cisco IOS Release 12.4(2)XB6, page 10
- Cisco MWAM Caveats, with Cisco IOS Release 12.4(2)XB6, page 15
- Related Documentation, page 16
- Documentation Roadmap for Implementing GGSN Release 6.0 on the Cisco MWAM, page 18

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

- Obtaining Documentation, page 19
- Documentation Feedback, page 20
- Obtaining Technical Assistance, page 20
- Obtaining Additional Publications and Information, page 22

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:

- 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)XB6 and includes the following sections:

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

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.4(2)XB6

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.XB6.bin	128MB	1 GB	RAM

Hardware and Software Requirements

Proper implementation of the Cisco GGSN features in the Cisco IOS Release 12.4(2)XB6 software requires the following hardware and software:

- Catalyst 6500/Cisco 7600 with a Cisco Supervisor Engine 720 and third-generation policy feature card (PFC3BXL) with integrated Multilayer Switch Feature Card 3 (MSFC3). The MSFC3s must be running the same Cisco IOS software release. The required release is Cisco IOS Release 12.2(18)SXE and later.

  For information about Cisco IOS Release 12.2(18)SXE, refer to the documentation on Cisco IOS Release 12.2 SX New Features available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/index.htm ware/ios122/122newft/122limit/122sx/index.htm

  For information about Cisco IOS Release 12.2(18)SXE, refer to the documentation on Cisco IOS Release 12.2 SX New Features available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/index.htm ware/ios122/122newft/122limit/122sx/index.htm

- Cisco Multi-Processor WAN Application Module (MWAMs) with the 1 GB memory option.

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.

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)XB6, 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*.

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)XB6, observe the following:

- The number of 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
```

For implementation of a service-aware GGSN (GGSN Release 5.2 and later), the following additional important notes, limitations, and restrictions apply:

- 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)XB6, page 7
- New and Changed Information in Cisco IOS Release 12.4(2)XB5, page 9
- New and Changed Information in Cisco IOS Release 12.4(2)XB4, page 9
- New and Changed Information in Cisco IOS Release 12.4(2)XB3, page 9
- New and Changed Information in Cisco IOS Release 12.4(2)XB2, page 10
- New and Changed Information in Cisco IOS Release 12.4(2)XB1, page 10
- New and Changed Information in Cisco IOS Release 12.4(2)XB, page 10

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, counters are set back to zero. However, this statement is incorrect. Please note that some counters, such as "cgprsAccPtSuccMsActivatedPdps," are not set back to zero.

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

Configuring Diameter/DCCA Interface Support

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

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

Configuring the DCCA Client Process on the GGSN

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

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

Command	Purpose
`Router(config-dcca-profile)# ccfh {continue | terminate | retry_terminate}`	Configures the default Credit Control Failure Handling (CCFH) action to take on PDP contexts when a fault condition occurs. • CONTINUE—Allows the PDP context and user traffic for the relevant category or categories to continue, regardless of the interruption. Quota management of other categories is not affected. • TERMINATE—Terminates the PDP context and the CC session. • RETRY—Allows the PDP context and user traffic for the relevant category or categories to continue. The DCCA client retries to send the CRR to an alternate server and if a failure-to-send condition occurs with the alternate server, the PDP context is terminated. The default is terminate. 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. • **continue**—Allows the PDP context and user traffic for the relevant category or categories to continue, regardless of the interruption. Quota management of other categories is not affected. • **terminate**—Terminates the PDP context and the CC session. • **retry_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. 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. The default is terminate. 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, counters are set back to zero. However, this statement is incorrect. Please note that some counters, such as "cgprsAccPtSuccMsActivatedPdps," are not set back to zero.

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

The ccfh Command Description

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

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

retry_terminate	Allows the PDP context and user traffic for the relevant category (or categories) to continue, regardless of the interruption while the DCCA client sends the 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. 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

This 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 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(2)XB6

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 types of caveats for the current Cisco IOS maintenance release:

- Open Caveats, page 11
- Resolved Caveats, page 11

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.

Using the Bug Navigator II

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.

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.

- 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

- 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.

Cisco MWAM Caveats, with Cisco IOS Release 12.4(2)XB6

This section lists the Cisco MWAM caveats that are open and resolved with Cisco 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.

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 17
- Platform-Specific Documents, page 17
- Cisco IOS Software Documentation Set, page 18

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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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(2)XB6