Release Notes for GGSN Release 6.0 on the Catalyst 6000 / Cisco 7600 MWAM for Cisco IOS Software Release 12.4(2)XB1

January 30, 2006

Cisco IOS Release 12.4(2)XB1

OL-5266-18

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)XB1. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4(2)XB1, see the "Caveats with Cisco IOS Release 12.4(2)XB1" section on page 7 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.

Documentation Survey

Is Cisco documentation helpful? Click here to give us your feedback or go to the following URL to give us your feedback:
http://www.cisco.com/warp/public/732/docsurvey/rtg/ to give us your feedback .

Contents

These release notes describe the following topics:

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

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

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)XB1 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)XB1

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco MWAM on Catalyst 6500 / Cisco 7600	GGSN Standard Feature Set	c6svcmwam-g8is-mz.124-2.XB1.bin	48MB	1 GB	RAM

Hardware and Software Requirements

Proper implementation of the Cisco GGSN features in the Cisco IOS Release 12.4(2)XB1 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

- At least one Cisco Multi-Processor WAN Application Module (MWAMs) in each Cisco 7600 series routers, each with the 1 GB memory option. The MWAMs must be running the same Cisco GGSN software release.

  Note Cisco 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-G4JS-M), Version 12.4(2)XB1, 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)XB1, 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 Cisco IOS image 12.3(14)YQ5 image can be loaded onto the MWAM.
- The same image must be loaded onto all processor complexes on the MWAM.
- The session console is provided by a TCP connection from the Supervisor module (no direct console).
- The 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 with Cisco GGSN Release 5.2 and later, the following additional important notes, limitations, and restrictions apply:

- RADIUS accounting is enabled between the CSG and GGSN to populate the Known User Entries Table (KUT) entries with the PDP context user information.
- CSG must be configured with the 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 the new implementations and behavior changes in the Cisco IOS Release 12.4 XB releases:

- New Implementations and Behavior Changes in Cisco IOS Release 12.4(2)XB1, page 7
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(2)XB, page 7

New Implementations and Behavior Changes in Cisco IOS Release 12.4(2)XB1

There are no new implementations or changes in behavior in the Cisco IOS Release 12.4(2)XB1 release of Cisco GGSN Release 6.0.

New Implementations and Behavior Changes 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

Caveats with Cisco IOS Release 12.4(2)XB1

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 8
- Resolved Caveats, page 11
- Unreproducible Caveat, page 13
- Closed Caveat, page 14

All caveats in Cisco IOS Release 12.4 and Cisco IOS Release 12.4 T are also in Cisco IOS Release 12.4(2)XB1.

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

This section documents possible unexpected behavior by Cisco IOS Release 12.4(2)XB1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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 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.

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(2)XB1

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

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

- 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 16
- Platform-Specific Documents, page 17
- Cisco IOS Software Documentation Set, page 17

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.