



Release Notes for GGSN Release 5.2 on the Catalyst 6000 / Cisco 7600 MWAM for Cisco IOS Software Release 12.3(14)YQ8

August 21, 2006

Cisco IOS Release 12.3(14)YQ8

These release notes for the Cisco Gateway GPRS Support Node (GGSN) Release 5.2 on the Cisco Multi-processor WAN Application Module (MWAM) describe the enhancements provided in Cisco IOS Release 12.3(14)YQ8. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(14)YQ8, see the “[Caveats with Cisco IOS Release 12.3\(14\)YQ8](#)” section on page 9 and *Caveats for Cisco IOS Release 12.3 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 12.3* located on Cisco.com and the Documentation CD-ROM.

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:

- [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](#)



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

- [New and Changed Information, page 7](#)
- [Caveats with Cisco IOS Release 12.3\(14\)YQ8, page 9](#)
- [Cisco MWAM Caveats with Cisco IOS Release 12.3\(14\)YQ8, page 13](#)
- [Related Documentation, page 16](#)
- [Documentation Roadmap for Implementing GGSN Release 5.2 on the Cisco MWAM, page 18](#)
- [Obtaining Documentation, page 19](#)
- [Documentation Feedback, page 20](#)
- [Obtaining Technical Assistance, page 20](#)
- [Obtaining Additional Publications and Information, page 21](#)

Introduction to Cisco GGSN on the Cisco MWAM

The following sections describe Cisco GGSN and the Catalyst 6500 / Cisco 7600 MWAM.

- [Cisco GGSN Overview, page 2](#)
- [Cisco MWAM Overview, page 3](#)

Cisco GGSN Overview

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

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

GPRS introduces the following two new major network elements:

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

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

Cisco MWAM Overview

With Cisco IOS Software Release 12.3(2)XB and later, the 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_1cn.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 12.3(14)YQ8 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 12.3(14)YQ2

| 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.123-14.YQ8.bin | 128 MB | 1 GB | RAM |

Hardware and Software Requirements

Proper implementation of the Cisco GGSN features in the Cisco IOS Release 12.3(14)YQ8 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>

- Cisco MWAM, with the 1 GB memory option, in each Cisco 7600 series router. If multiple MWAMs are used, the MWAMs must be running the same Cisco GGSN software release.



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.

- IPsec VPN card (if security is a requirement)
- A Cisco Content Services Gateway (CSG) module in each of the Cisco 7600 series routers. The CSGs must be running the same Cisco CSG software release, Release 3.1(3)C6(1) or later.



Note

A Hardware-Software Compatibility Matrix is available on CCO for users with CCO login accounts. This matrix allows users to search for supported hardware components by entering a Cisco platform and IOS Release. The Hardware-Software Compatibility Matrix tool is available at the following URL:

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hswmatrix.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 12.3(14)YQ8, 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 12.3(14)YQ8, 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, 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 $N3 \times T3$ must be greater than:

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

where:

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

New and Changed Information

The following section lists the new implementations and behavior changes in the Cisco IOS Release 12.3 YQ releases:

- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YQ8, page 7](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YQ7, page 7](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YQ6, page 7](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YQ5, page 7](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YQ4, page 7](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YQ3, page 7](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YQ2, page 8](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YQ1, page 8](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YQ, page 8](#)

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YQ8

There are no new implementations or behavior changes in Cisco IOS Release 12.3(14)YQ8.

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YQ7

There are no new implementations or behavior changes in Cisco IOS Release 12.3(14)YQ7.

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YQ6

There are no new implementations or behavior changes in Cisco IOS Release 12.3(14)YQ6.

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YQ5

There are no new implementations or behavior changes in Cisco IOS Release 12.3(14)YQ5.

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YQ4

There are no new implementations or behavior changes in Cisco IOS Release 12.3(14)YQ4.

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YQ3

There are no new implementations or behavior changes in Cisco IOS Release 12.3(14)YQ3.

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YQ2

With this release of the Cisco GGSN software, after a packet data protocol (PDP) context is established, subsequent create PDP context requests are no longer treated as update requests (update of parameters such as quality of service [QoS], SGSN, etc. on an existing PDP). Instead, as specified by TS 29.060 CR311, the default behavior for GTPv1 PDPs is as follows:

- If a create PDP context request with a tunnel end-point identifier (TEID) of 0 is received on an existing PDP context, the GGSN tears down the existing context and all associated secondary PDPs locally, and processes the new request.
- If a create PDP context request with a TEID of non-zero is received on an existing PDP context, the GGSN rejects the create PDP context request with a “service not supported” cause code and deletes the PDP context.

Therefore, in GGSN Release 5.2, Cisco IOS Release 12.3(14)YQ2 and later, the **gprs gtp create-request v1 update-existing-pdp** global configuration command that configures the “create-as-update” behavior, is obsolete.

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YQ1

There are no new implementations or behavior changes in Cisco IOS Release 12.3(14)YQ1.

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YQ

Cisco GGSN Release 5.2, Cisco IOS Release 12.3(14)YQ and later supports, in conjunction with the Cisco CSG and Cisco Diameter/DCCA support, real-time credit-control for prepaid users and service-aware billing for postpaid and prepaid users.

The GGSN and CSG together, function as a service-aware GGSN. The CSG categorizes traffic, reports usage, and management quota. The GGSN provides a Diameter interface to the Diameter Credit Control Application (DCCA) server for the CSG to request quota and report usage.

The GGSN maintains all PDP contexts and determines if they are prepaid or postpaid. If service-based charging is required (prepaid or postpaid), entries are created on the CSG. The CSG inspects the service categories and reports usage back to the GGSN. If the user is to be treated as a prepaid user (online charging), the GGSN translates usage sent from the Cisco CSG and sends it to a DCCA server. If the user is to be treated as a postpaid user (offline charging), the GGSN records usage information reported by the Cisco CSG in enhanced G-CDRs.

For information the features in GGSN Release 5.2, see the Cisco IOS Release 12.3(14)YQ Cisco GGSN Release 5.2 configuration guide and command reference:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123yq/index.htm>

Caveats with Cisco IOS Release 12.3(14)YQ8

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 only open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T are also in Cisco IOS Release 12.3(14)YQ8.

For information on caveats in Cisco IOS Release 12.3, see *Caveats for Cisco IOS Release 12.3*.

For information on caveats in Cisco IOS Release 12.3 T, see *Caveats for Cisco IOS Release 12.3T*, 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 12.3(14)YQ8 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg03019

Description: 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.

- CSCei87444

Description: A heavy traffic load might cause a Cisco GGSN that is running an encrypted image to reload. This condition only occurs when the CPU usage is consistently over 96 percent for extended periods of time, and bi-directional data is being sent over all IPSec tunnels simultaneously, causing the IPSec card to reset.

Workaround: Configuring policing in such a way that high unchecked data is not sent for extended periods of time.

- 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 International Mobile Subscriber Identity (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.

- CSCse95622

Description: The SGSN address is not present in some R99 partial G-CDRs. This condition occurs if the following GGSN configuration is used:

- the **gprs charging release 99** global configuration command is configured
- the **gprs charging cdr-option no-partial-cdr-generation** global configuration command is configured

and one of the following is configured:

- **gprs charging container sgsn-change-limit** global configuration command
- **limit sgsn-change** charging profile configuration command

If the G-CDR is closed due to any trigger other than an SGSN change limit, the first G-CDR after the change will contain the value for the SGSN address, but in subsequent G-CDRs, the SGSN address will not be present.

Workaround: To ensure that the SGSN address value is present in all G-CDRs, configure the **gprs charging cdr-option no-partial-cdr-generation all** global configuration command.

Resolved Caveats

The caveats listed in this section are resolved in Cisco IOS Release 12.3(14)YQ8. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek26492

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

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

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

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

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

- CSCek37177

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

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

This issue is documented as Cisco bug ID [CSCek37177](#).

There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>

- CSCek49375

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

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

- CSCek50950

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

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

- CSCek51987

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

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

- CSCin99850

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

- CSCsa53334

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

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

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

This advisory is posted at:

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

- CSCsb06658

A vulnerability exists in certain Cisco IOS software release trains running on the Cisco IAD2400 series, Cisco 1900 series Mobile Wireless Edge Routers and Cisco VG224 Analog Phone Gateways. Vulnerable versions may contain a default hard-coded Simple Network Management Protocol (SNMP) community string when SNMP is enabled on the device. The default community string is a result of inadvertently identifying these devices as supporting Data Over Cable Service Interface Specification (DOCSIS) compliant interfaces. The consequence of this error is that an additional read-write community string may be enabled if the device is configured for SNMP management, allowing a knowledgeable attacker the potential to gain privileged access to the device.

Cisco is making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060920-docsis.shtml>.

- CSCsd76596

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

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

- CSCse62599

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

- CSCse64581

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

- CSCse66427

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

 - a. A GTPv0 PDP context is created.
 - b. When the **show gprs gtp status** command is issued on the standby GGSN, the counter for the prepaid PDP counter displays an incorrect value.
 - c. The GTPv0 PDP context is deleted.
 - d. The counter on the standby GGSN for the for the prepaid PDP now displays a very large and incorrect value when the **show gprs gtp status** command is issued.
- CSCse79433

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

Cisco MWAM Caveats with Cisco IOS Release 12.3(14)YQ8

This section lists the Cisco MWAM caveats that are open and resolved with Cisco Release 12.3(14)YQ8.

Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.3(14)YQ8:

- 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 sabyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

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

- CSCej07438

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

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

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

- CSCsa50215

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

Workaround: Configure the **ip rcmd rcp-enabled** command on the supervisor module. For supervisor release SXF4 and later, also configure the **ip rcmd remote-host localuser MWAM EOBC address remoteuser enable** command on the supervisor for each MWAM processor. For the supervisor config-mode to work, this remote IP address has to be not just any IP, but the EOBC address(127.0.0.xy, where x equals slot and y equals processor). For example, for MWAM slot 10, processor 2, configure **ip rcmd remote-host * 127.0.0.102 * enable**.

- CSCsb59293

Description: When the MWAM is in Supervisor configuration mode, if the configuration stored on the Supervisor fails to update, the local startup configuration might still be updated. This causes the wrong configuration to display when the **show startup-config** command is executed. When the MWAM is reloaded, it attempts to load configurations from 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.

- 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 supervisor configuration mode is set from the PC using the **boot mode** command.

Workaround: Change the configuration mode from the MWAM IOS instance using the **mwam config-mode** command.

- CSCse28123

Description: When the **write memory** command is issued, the supervisor might crash.

Workaround: There is currently no known workaround.

- CSCse67478

Description: When reloading one MWAM processor of an MWAM complex, the second processor does not send a RADIUS Accounting OFF. This condition occurs when you reload an MWAM processor part of an MWAM complex. An MWAM complex consists of two MWAM processors.

Workaround: Have a script on the RADIUS server to correlate the NAS IP-address of both MWAM processors that belong to the same complex. Consider that if one RADIUS Accounting OFF is received, the other MWAM processor also has been reloaded.

Resolved Caveats

There are no newly resolved Cisco MWAM caveats for Cisco IOS Release 12.3(14)YQ8.

Documentation Updates

In reference to the charging profile index AAA attribute, the following note was added to the “Configuring Charging Profiles” section of the “Configuring Charging on the GGSN” chapter of the *Cisco GGSN Release 5.2 Configuration Guide*.



Note

The charging profile index received from AAA will take effect only if service-awareness has been configured globally on the GGSN (using the **gprs service-aware** global configuration command), and at the APN level (using the **service-aware** access-point configuration command). For information on configuring a service-aware GGSN, see the “Configuring Enhanced Service-Aware Billing” chapter of the *Cisco GGSN Configuration Guide*.

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 Cisco.com:

- *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 12.3*

On Cisco.com at:

Technical Support & Documentation: Technical Support & Documentation: Cisco IOS Software: Cisco IOS Releases 12.3 Mainline: Release Notes:

- *Caveats for Cisco IOS Release 12.3 T*

See *Caveats for Cisco IOS Release 12.3* and *Caveats for Cisco IOS Release 12.3T*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.3 and Release 12.3 T.

On Cisco.com at:

Technical Support & Documentation: Technical Support & Documentation: Cisco IOS Software: Cisco IOS Releases 12.3 T: Release Notes



Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. You can 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 Cisco.com at:

Technical Support & Documentation: Technical Support & Documentation: Cisco IOS Software: Cisco IOS Releases 12.3 Mainline: Product Literature

Technical Support & Documentation: Technical Support & Documentation: Cisco IOS Software: Cisco IOS Releases 12.3 T: Product Literature

Technical Support & Documentation: Technical Support & Documentation: Cisco IOS Software: Cisco IOS Releases 12.3 Special and Early Deployments: Product Literature

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.

OnCisco.com, two master hot-linked documents provide information for the Cisco IOS software documentation set.

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

Release 12.3 Documentation Set

You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at:

Technical Support & Documentation: Technical Support & Documentation: Cisco IOS Software



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 5.2 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

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 5.2 feature and configure the GGSNs on the MWAM:

- Cisco GGSN 5.2 Configuration Guide and Command Reference for Cisco IOS Release 12.3(14)YQ.
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_inpk/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.ht>

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

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Copyright © 2003-2006, Cisco Systems, Inc.
All rights reserved.