



Release Notes for Cisco GGSN Release 8.0 on the Cisco SAMI, Cisco IOS Software Release 12.4 XQ Releases

Latest Publication Date: August 1, 2011

Last Publication Date: February 23, 2011

Cisco IOS Release 12.4(15)XQ8

These release notes for the Cisco Gateway GPRS Support Node (GGSN) Release 8.0 on the Cisco Service and Application Module for IP (SAMI) describe the enhancements provided in Cisco IOS Release 12.4(15)XQ8. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4 XQ releases, see the [“Caveats” section on page 14](#) and *Caveats for Cisco IOS Release 12.4 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

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

Technical Documentation Ideas Forum

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

Contents

These release notes describe the following topics:

- [Introduction to Cisco GGSN on the Cisco SAMI, page 2](#)
- [System Requirements, page 3](#)
- [MIBs, page 5](#)
- [Limitations, Restrictions, and Important Notes, page 6](#)
- [New and Changed Information, page 8](#)



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

© 2011 Cisco Systems, Inc. All rights reserved.

- [Caveats, page 14](#)
- [Related Documentation, page 52](#)
- [Documentation Roadmap for Implementing GGSN Release 8.0 on the Cisco SAMI, page 53](#)
- [Obtaining Documentation and Submitting a Service Request, page 54](#)

Introduction to Cisco GGSN on the Cisco SAMI

The following sections describe the Cisco Gateway GPRS Support Node (GGSN) and the Cisco Service and Application Module for IP (SAMI).

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

Cisco GGSN Overview

The Cisco 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. The Cisco GPRS solution enables mobile wireless service providers to supply their mobile subscribers with packet-based data services in GSM networks.

GPRS introduces the following two new major network elements:

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

Cisco SAMI Overview

With Cisco IOS Software Release 12.4(15)XQ or later, Cisco GGSN software runs on the Cisco SAMI installed in a Cisco 7600 series router.

The SAMI, with its six Power PCs (PPCs) running at 1.25 GHz, each of which can run an instance of the same Cisco mobile wireless application image, offers a parallel architecture for Cisco mobile wireless applications such as the Cisco Content Services Gateway - 2nd Generation (CSG2), the Cisco Mobile Wireless Home Agent Feature, and with Cisco IOS Release 12.4(15)XQ release or later, the Cisco Gateway GPRS Support Node, Release 8.0.

The benefits of the SAMI architecture include:

- Increased processing power and session density
- Reduced inter-CPU data sharing
- Separation of the control and the data plane
- Improved management capabilities

- Less complex to configure
- Easier debugging

The SAMI does not provide external ports but is connected to the switch fabric in the Cisco 7600 series router chassis. An internal Gigabit Ethernet port provides an interface between SAMI and the Supervisor module. Virtual Local Area Networks (VLANs) direct traffic from external ports via the Supervisor module to each instance of the Cisco IOS mobile wireless application running on the PPCs.

Through the supervisor module, a session to each application on a SAMI in a chassis can be established. Each session can be used for configuring, monitoring, and troubleshooting Cisco IOS mobile wireless application running on the SAMI PPCs.

For information on establishing sessions to Cisco IOS mobile wireless applications running on the SAMI PPCs, refer to the *Cisco Service and Application Module for IP User Guide*:

http://www.cisco.com/en/US/docs/wireless/service_application_module/sami/user/guide/samiv1.html



Note

Each Cisco application on a SAMI PPC must be configured individually, however, the SAMI remote console and logging (RCAL) feature enables operators to use the supervisor engine console as a single connection point from which to access the Cisco SAMI line card control processor (LCP) and the PPCs on the SAMI to control debugging, display **show** commands, and view logging output for the PPCs on the SAMI.

The software bundle that provides the Cisco IOS mobile wireless application is downloaded through the supervisor engine module and distributed to each PPC on the SAMI. The same image is automatically installed on all the PPCs in the SAMI.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(15)XQ and includes the following sections:

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

Memory Recommendations

Table 1 *Images and Memory Recommendations for Cisco IOS Release 12.4(15)XQ*

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco SAMI/ Cisco 7600	GGSN Standard Feature Set	c7svcsami-g8ik9s-mz.124-15.XQ8.bin	128 MB	2 GB	RAM

Hardware and Software Requirements

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

- Any module that has ports to connect to the network.
- One of the following Cisco 7600 series routers and supervisor engines running Cisco IOS Release 12.2(33)SRC or later:
 - Cisco 7600 Series Supervisor Engine 720 with a Multiplayer Switch Feature Card 3 (WSSUP720)
 - Cisco 7600 Series Supervisor Engine 720 with a Multilayer Switch Feature Card 3 and Policy Feature Card 3B (WS-SUP720-3B)
 - Cisco 7600 Series Supervisor Engine 720 with a Multilayer Switch Feature Card 3 and Policy Feature Card 3BXL (WS-SUP720-3BXL)
 - Cisco 7600 Series Supervisor Engine 32 with a Multiplayer Switch Feature Card (WS-SUP32-GE-3B) with LCP ROMMON Version 12.2(121) or later on the Cisco SAMI.
 - Cisco 7600 Series Supervisor Engine 32 with a Multilayer Switch Feature Card and 10 Gigabit Ethernet Uplinks (WS-SUP32-10GE-3B) with LCP ROMMON Version 12.2[121] or later on the Cisco SAMI.

For details on upgrading the Cisco IOS release running on the supervisor engine, refer to the “Upgrading to a New Software Release” section in the Release Notes for Cisco IOS Release 12.2SR. For information about verifying and upgrading the LCP ROMMON image on the Cisco SAMI, refer to the [Cisco Service and Application Module for IP User Guide](#).



Note The Cisco IOS software required on the supervisor engine is dependent on the supervisor engine being used and the Cisco mobile wireless application running on the Cisco SAMI processors.

- Cisco Service and Application Module for IP (Cisco Product Number: WS-SVC-SAMI-BB-K9). The SAMI processors must be running Cisco IOS Release 12.4(15)XQ or later. The image is automatically loaded onto each processor during an image upgrade and supports both the 1 GB memory default and the 2 GB memory option (Cisco Product Number: MEM-SAMI-6P-2GB[=]).
- IPSec VPN Services Module (for security)



Note

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

GTP-Session Redundancy

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

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

Enhanced Service-Aware Billing

In addition to the required hardware and software, implementing enhanced service-aware billing requires an additional Cisco SAMI running the Cisco Content Services Gateway - 2nd Generation software in each Cisco 7600 series router.

GTP APN-Aware Server Load Balancing

Support for GTP access point name (APN)-aware SLB requires Cisco IOS Release 12.2(33)SRB1 or later on the supervisor engine module.

Determining the Software Version

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

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) SAMI Software (g8ik9s), Version 12.4(15)XQ8, EARLY DEPLOYMENT RELEASE SOFTWARE
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 the Cisco SAMI Software

For information on upgrading the Cisco SAMI software, see to the *Cisco Service and Application Module for IP User Guide*:

http://www.cisco.com/en/US/docs/wireless/service_application_module/sami/user/guide/samiv1.html

**Note**

The image download process loads the Cisco IOS image onto the six processors on the SAMI.

MIBs

Current MIBs

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

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

Limitations, Restrictions, and Important Notes

When configuring the Cisco GGSN, observe the following:

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



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

Table 2 lists the maximum number of PDP contexts the Cisco SAMI with the 1 GB memory option can support. Table 3 lists the maximum number the Cisco SAMI with the 2 GB memory option can support.:

Table 2 *Number of PDPs Supported in 1 GB SAMI*

PDP Type	Maximum Number per GGSN	Maximum Number per SAMI ¹
IPv4	64,000	360,000
IPv6	8,000	48,000
PPP Regeneration	16,000	96,000
PPP	8,000	48,000

1. Maximum number per SAMI on which six GGSNs are configured.

Table 3 *Number of PDPs Supported in 2 GB SAMI*

PDP Type	Maximum Number per GGSN	Maximum Number per SAMI ¹
IPv4	136,000	816,000
IPv6	16,000	96,000
PPP Regeneration	32,000	192,000
PPP	8,000	48,000

1. Maximum number per SAMI on which six GGSNs are configured.

- 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 Hot Standby Router Protocol (HSRP) 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, the following additional important notes, limitations, and restrictions apply:

- Enable Remote Authentication Dial-In User Service (RADIUS) accounting between the Cisco CSG2 and GGSN to populate the Cisco CSG2 User Table entries with the PDP context user information.
- Configure the Cisco CSG2 with the QS addresses of all of the GGSN instances.
- Configure the Service IDs on the Cisco CSG2 as numeric strings that match the category IDs on the Diameter Credit Control Application (DCCA) server.
- If RADIUS is not being used, configure the Cisco CSG2 as a RADIUS endpoint on the GGSN.
- On the SGSN, ensure that configure the values for the number GTP N3 requests and T3 retransmissions larger than the sum of all possible server timers (RADIUS, DCCA, and CSG2).

Specifically the SGSN $N3 * T3$ must be greater than:

$$2 \times \text{RADIUS timeout} + N \times \text{DCCA timeout} + \text{CSG2 timeout}$$

where:

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



Note Configuring a $N3 * T3$ lower than the default might impact slow TCP-based charging paths.

New and Changed Information

The following section lists the new implementations and behavior changes in the Cisco IOS Release 12.4 XQ releases:

- [New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ8, page 8](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ7, page 9](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ6, page 9](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ5, page 10](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ4, page 10](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ3, page 10](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ2, page 11](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ1, page 11](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ, page 11](#)

For detailed information about the new and existing features in GGSN Release 8.0, see the *Cisco GGSN Release 8.0* configuration guide and command reference accessible from:

http://www.cisco.com/en/US/products/sw/wirelssw/ps873/tsd_products_support_series_home.html

New Implementations and Behavior Changes in Cisco IOS Release 12.4(15)XQ8

Cisco IOS Release 12.4(15)XQ8 introduces “Throttling GTP Request Re-Enqueues” support to Cisco GGSN Release 8.0.

If there is a GTP request that the Cisco GGSN needs to service for an existing PDP context, and a pending request for that PDP context already exists, the GGSN cannot immediately service the new request.

In some cases the GTP request is re-enqueued in the GTP queue until the PDP is ready to be updated/created. Ideally, the GGSN should service all such GTP requests within a few re-enqueues, however, if for some reason it cannot, and a request is continuously re-queued, the GGSN attempts to process the same request again and again, which causes a very high CPU.

To prevent requests from being process again and again, you can throttle the number of times a GTP request can be re-enqueued.

To configure the number of times a GTP request can be re-enqueued in the GTP queue, use the following command while in global configuration mode:

Command	Purpose
Router(config)# gprs gtp request re-enqueue num	Configures the number of times a GTP request can be re-enqueued in the GTP queue. A valid value is a number between 1 and 1000. The default is 10.

Using the **no** form of this command resets the value to the default (10).



Note

You can modify this command dynamically, regardless of the number of existing PDPs, and the command is immediately effective.

To display re-enqueue statistics, use the following command while in privileged EXEC mode:

Command	Purpose
Router# show gprs gtp request re-enqueue statistics	Displays the re-enqueue statistics, including the number of times GTP requests are re-enqueued the first time, the total number of times requests are re-enqueued, and the number of requests dropped.

For example, issuing the **show gprs gtp request re-enqueue statistics** command displays the following:

```
GGSN# show gprs gtp request re-enqueue statistics
  GTP Req re-enqueue first_time 1          GTP Req re-enqueue total      1
  GTP Req re-enqueue dropped      1
GGSN#
```

To clear the re-enqueue statistics counters, use the following command while in privileged EXEC mode:

Command	Purpose
Router# clear gprs gtp request re-enqueue statistics	Clears the counters for the re-enqueue statistics.

When configuring the GTP request re-enqueue throttle, note the following:

- If a GTP request is re-enqueued for the configured or default value, the following debug messages display to indicate the same when **debug gprs gtp errors** is enabled:

```
SAMI 1/4: Jul  5 22:06:21.079: GPRS:1231230000000010:A GTP Req Packet has reached
limit 0 for re-enqueue. Queue GTP msg, Re-enqueue reason:Delete Before Recreate
SAMI 1/4: Jul  5 22:06:21.079: GPRS:1231230000000010:TID: 1231230000000010, PDP
Internal Flags:40440001, PDP Update Flags:00000000, PDP Delete Flags:00000000, MCB
Flags:00020008, APN: mani.com, Packet App flags 00000000, PDP:0x425B767C, MCB
0x4A423534
```

- The **show gprs gtp request re-enqueue statistics** privileged EXEC command is also available under the **show tech** privileged EXEC command.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(15)XQ7

There are no new implementations or behavior changes in Cisco IOS Release 12.4(15)XQ7.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(15)XQ6

There are no new implementations or behavior changes in Cisco IOS Release 12.4(15)XQ6.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(15)XQ5

The following global configuration command has been added to configure the Cisco GGSN behavior when it receives a T-PDU for a GTPv1 PDP context without a sequence number in the GTPv1 header:

```
[no] gprs gtp tpdu reorder-required sequence receive mandatory
```

When the **gprs gtp tpdu reorder-required sequence receive mandatory** command is configured, when the GTPv1 PDP has `reorder_required` set to TRUE, if a GTPv1 T-PDU without a sequence number (`s=0`) is received by the Cisco GGSN, the T-PDU is considered an out-of-sequence T-PDU and is dropped.

By default this command is not configured, and the default behavior is when the GTPv1 PDP context has `reorder_required` set to TRUE, if a GTPv1 T-PDU without a sequence number (`s=0`) is received by the Cisco GGSN, the T-PDU is allowed and treated as a valid T-PDU, which does not require reordering and sequence number checks.

If the PDP context has `reorder_required` set to FALSE, the T-PDU is accepted without any check for sequence number (both `s=0` and `s=1` are accepted in this case). This is an existing behavior and has not changed in Cisco IOS Release 12.4(15)XQ5.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(15)XQ4

To ensure that the most recent Long Sequence Record Number (LSRN) ID value is used in charging records, before downgrading from Cisco IOS Release 12.4(15)XQ4 or later to Cisco IOS Release 12.4(15)XQ3, XQ2, XQ1, or XQ, or before upgrading from Cisco IOS Release 12.4(15)XQ4 to Cisco GGSN Release 9.0, Cisco IOS Release 12.4(22)YE or YE1, execute the **sami sync-nvvar ios-to-rommon** privileged EXEC command at each of the PPC consoles.



Note

The **sami sync-nvvar ios-to-rommon** command has to be issued only once before upgrading or downgrading an image.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(15)XQ3

Prior to Cisco IOS Release 12.4(15)XQ3, when the Cisco GGSN received a Transport (T-PDU) without a sequence number in the GTPv1 header (`s bit=0`), it dropped the T-PDU. With Cisco IOS Release 12.4(5)XQ3, the new default behavior is to allow T-PDUs without a sequence number.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(15)XQ2

The following behavior change is introduced in Cisco GGSN Release 8.0, Cisco IOS Release 12.4(15)XQ2.

- **Generating Pure ASN.1 Records**

With Cisco IOS 12.4(15)XQ2 or later, the feature functionality to send charging records to Small Computer Systems Interface over IP (iSCSI) has been enhanced to send either the GTP or the pure ASN.1 mode. ASN.1 mode writes the charging record from the Call Event Record type onward. To enable the GGSN to generate pure ASN.1 records, the data record format needs to be configured using the **gprs charging iscsi rec-format asn.1** global configuration command.



Note The records in this format are generated only when auto-retrieval is disabled on the GGSN, which is the default behavior. This configuration should be used only when charging records are stored only on an iSCSI target (the charging gateway should not be configured in this case).

New Implementations and Behavior Changes in Cisco IOS Release 12.4(15)XQ1

There are no new implementations or behavior changes in Cisco IOS Release 12.4(15)XQ1.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(15)XQ

The following behavior change exists in Cisco GGSN Release 8.0, Cisco IOS Release 12.4(15)XQ and later:

- The Cisco GGSN does not support the Cisco Express Forwarding (CEF) neighbor resolution optimization feature, which is enabled by default.

Therefore, to avoid the possibility of incomplete adjacency on VLAN interfaces for the redirected destination IP address and an impact to the upstream traffic flow for PDP sessions upon bootup, ensure that you configure the **no ip cef optimize neighbor resolution** command.

Support for the following new features is introduced in Cisco GGSN Release 8.0, Cisco IOS Release 12.4(15)XQ. For detailed information on each of these features, see the *Cisco GGSN Release 8.0 Configuration Guide*.

- **GGSN-Initiated Update PDP Context Requests**

With this release, a Cisco GGSN can send an Update PDP Context Request (as defined in 3GPP TR 29.060 v7.5.1, section 7.3.3) to an SGSN to negotiate the quality of service (QoS) of a PDP context.

An external entity, such as the Cisco Content Services Gateway (CSG) in an Gx environment, can push a new QoS profile to the GGSN to apply on a particular PDP context. The GGSN then pushes the changes to the RAN in an Update PDP Context Request to the SGSN.

Additionally, when a direct tunnel is being used for a PDP context, the GGSN sends an Update PDP Context Request to an SGSN in response to an error indication message from a Radio Network Controller (RNC).

- **RADIUS Change of Authorization Message**

The RADIUS Change of Authorization (CoA) message contains information for dynamically changing session authorizations. With this release, the Cisco GGSN utilizes the base Cisco IOS Authentication, Authorization, and Accounting (AAA) to support the RADIUS CoA message, as defined by RFC 3576, but with an additional 3GPP QoS attribute specific to the Cisco GGSN and Cisco CSG2 interface that indicates the updated QoS and the Acct-Session-ID to identify the PDP context.

- **Downloadable QoS Profile**

If an APN is configured in non-transparent mode, a user is authenticated before the PDP context is created. GGSN sends an access-request to AAA server with parameters in the user provided protocol configuration option (PCO), or using anonymous authentication if anonymous user is enabled on APN.

In the access-accept message from the RADIUS server, user-specific attributes such as the session and idle timeout values, can be downloaded and applied to the PDP context. In addition to these attributes, the Cisco GGSN supports downloading the QoS profile via the QoS VSA (as defined by 3GPP TS 24.008). If a 3GPP QoS profile attribute is received from an AAA server in an access-accept message, the GGSN retrieves the attribute and applies it to the PDP context. If the attribute is not valid, or there is a format error in the attribute, the attribute is ignored and the SGSN requested QoS profile is used for QoS negotiation.

- **PPP-Regeneration Scalability**

This release of the Cisco GGSN allows PDPs regenerated to a PPP session to run on software interface description blocks (IDBs). Allowing PPP sessions to run on software IDBs, can increase the number of supported sessions.

- **AAA Enhancements**

Cisco GGSN Release 8.0 utilizes the base Cisco IOS AAA functionality introduced to provide support for the following:

- Simultaneous method list level broadcast and wait accounting
- Per-session timer for interim accounting records (periodic accounting timer)

- **Anonymous User Access for PPP-Regeneration**

Anonymous user access for PPP-regenerated PDPs is supported with Cisco GGSN Release 8.0 or later.

When the **anonymous user** access-point user configuration command is configured under an APN that is configured for PPP regeneration, the values configured for the username and password are used if the PCO information element is not included when the PDP context is created.

- **Downloadable Pool Name Support**

When the **ip-address-pool radius-client** access-point configuration command is configured under an APN, if an address pool name is received as a part of the Access-Accept message while authenticating the user, that address pool is used to assign the IP address to the mobile station. If the Access-Accept message also includes an IP address, the IP address takes precedent over the address pool name, and the IP address in the Access-Accept message is used instead of being allocated from the pool.

- **Direct Tunnel Support**

The Cisco GGSN supports direct tunnel PDPs. The direct tunnel functionality enables an SGSN to establish a direct user plane tunnel between the radio network controller (RNC) and a GGSN.

The SGSN functions as the gateway between the RNC and the core network, handling both signaling traffic to keep track of the location of mobile devices, as well as the actual data packets being exchanged between the mobile device and the Internet.

Currently a tunnel exists between the GGSN and the SGSN and another tunnel between the SGSN and the RNC. Therefore all data packets have to pass the SGSN, which has to terminate one tunnel, extract the packet, and put it into another tunnel. This process takes time and processing power. With direct tunnel support, the SGSN can create a direct tunnel between the RNC and the GGSN and no longer have to process data packets, but continue to manage location issues by modifying the tunnel if a mobile device moves to an area served by another RNC.

- **Changeable Charging Source Interface**

By default, the global GTP virtual template interface is used for all charging messages. With this release of the Cisco GGSN, you can configure a loopback interface, and configure the GGSN to use that loopback interface for all charging messages. This feature enables charging network traffic to be segregated into a VRF or private VLAN. Once the charging source interface is specified, the GTP path to the charging gateways will be recreated with the new address obtained from the loopback interface.

- **Suppressing Echo Requests per SGSN**

Echo requests can be disabled per SGSN and/or UDP port. This feature enables operators to selectively disable charging for GSNs that might not have the capability to respond to echo requests from the GGSN entirely, or only those echo requests received on certain UDP ports, while keeping the echo requests intact for the other SGSNs.

When a new path is created, the GGSN checks to see if the path parameters, namely the destination address and port, matches any of the conditions configured when suppressing echo requests. If the parameters match, the GGSN sets the path echo interval to 0 for that path. Otherwise, the global path echo interval configuration is used to send echo requests.

- **iSCSI Transport Protocol Support**

With Cisco GGSN Release 8.0 or later, you can configure the GGSN to backup G-CDRs to, and retrieve G-CDRs from, a storage target on a Storage Area Network (SAN) when a charging gateway is unavailable.

The Cisco GGSN utilizes the Cisco IOS software Small Computer Systems Interface over IP (iSCSI) support, as defined in RFC 3720, to enable G-CDR storage and retrieval from SAN storage.

Caveats

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

All caveats in Cisco IOS Release 12.4 and Cisco IOS Release 12.4 T are also in Cisco IOS Release 12.4(15)XQ.

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>.

This section lists the following:

- [Caveats - Cisco IOS Release 12.4\(15\)XQ8, page 15](#)
- [Caveats - Cisco IOS Release 12.4\(15\)XQ7, page 18](#)
- [Caveats - Cisco IOS Release 12.4\(15\)XQ6, page 21](#)
- [Caveats - Cisco IOS Release 12.4\(15\)XQ5, page 24](#)
- [Caveats - Cisco IOS Release 12.4\(15\)XQ4, page 27](#)
- [Caveats - Cisco IOS Release 12.4\(15\)XQ3, page 30](#)
- [Caveats - Cisco IOS Release 12.4\(15\)XQ2, page 36](#)
- [Caveats - Cisco IOS Release 12.4\(15\)XQ1, page 44](#)
- [Caveats - Cisco IOS Release 12.4\(15\)XQ, page 49](#)

Caveats - Cisco IOS Release 12.4(15)XQ8

This section contains the following types of caveats that pertain to Cisco IOS Release 12.4(15)XQ8:

- [Open Caveats, page 18](#)
- [Resolved Caveats, page 19](#)

Open Caveats

**Note**

Open caveats for a release also apply to the prior releases.

The following sections document possible unexpected behavior and describe only severity 1 and 2 caveats, and select severity 3 caveats.

- [Cisco GGSN Open Caveats, page 18](#)
- [Cisco SAMI Open Caveats, page 18](#)

Cisco GGSN Open Caveats

The following Cisco GGSN-specific caveat is open in Cisco IOS Release 12.4(15)XQ8.

- CSCtr10962

The Cisco SAMI running Cisco GGSN Release 8.0, Cisco IOS Release 12.4(15)XQ7 might experience high CPU utilization (greater than 97%) in the GTP management process because of stuck PDP contexts.

The high CPU condition could be triggered by a serving GPRS support node (SGSN) restart (PATH_RESTART) when there is a hung PDP context in the GGSN that belongs to the same SGSN (path).

This condition might occur with a enhanced GGSN (eGGSN) service aware implementation.

Workaround: Place the GGSN into maintenance mode by using the **gprs service-mode maintenance** command in global configuration mode, return the GGSN to operational mode by using the **gprs service-mode operational** command, and then reload the GGSN.

Cisco SAMI Open Caveats

There are no known Cisco SAMI caveats open with Cisco IOS Release 12.4(15)XQ8.

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(15)XQ8. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- [Cisco GGSN Resolved Caveats, page 19](#)
- [Cisco SAMI Resolved Caveats, page 20](#)

Cisco GGSN Resolved Caveats

This section lists the Cisco GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(15)XQ8.

- CSCso02147

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

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

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

Cisco has released free software updates that address these vulnerabilities.

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

- CSCsy75416

A Diameter Credit Control Application (DCCA) Credit Control Answer (CCA) update message sent to the GGSN with a manipulated Session ID causes the GGSN to crash.

- CSCth11006

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

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

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

Cisco has released free software updates that address these vulnerabilities.

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

- CSCti48483

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

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

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

Cisco has released free software updates that address these vulnerabilities.

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

- CSCtj04672

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

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

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

Cisco has released free software updates that address these vulnerabilities.

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

- CSCto70902

When a subscriber connects to an APN configured to support routing behind the mobile station (the **network-behind-mobile** access-point configuration command is configured), the Cisco GGSN sends an Access-Request to RADIUS and receives the framed-ip-route in return, as expected.

However, one of the framed routes is illegitimate according to the IANA IPv4 Address Space Registry. Once the invalid address is downloaded and installed, the same routing entry is added for every minute until the user disconnects the PDP. This occurs for only illegitimate subnets. Upon disconnecting the PDP, only one entry is deleted and the remaining entries remain present. This causes the memory consumption on the Cisco GGSN to continuously raise.

- CSCtq36777

In an enhanced GGSN (eGGSN) scenario, in which the Cisco GGSN and Cisco CSG2 are implemented together to provide service-aware billing, if the Diameter Credit Control Application (DCCA) server does not send the Volume/Time threshold in the Volume-Quota-Threshold AVP and the Time-Quota-Threshold AVP in a Credit Control Answer (CCA) to the quota server interface on the Cisco GGSN, the Cisco GGSN continues to dictate a Volume/Time threshold of zero (0) to the Cisco CSG2 via GTP', as seen below:

```
Granted Quadrans Quadrans: 1843200
Granted Quadrans Units: Bytes IP
Granted Quadrans Flags: 0x03
Granted Quadrans Threshold: 0
```

The 0x03 flag indicates that this is a dictated and mandatory value to which the Cisco CSG2 must comply.

This condition occurs when the DCCA server does not send a Volume/Time threshold value to the Cisco GGSN quota server interface. The Cisco GGSN sends a Volume/Time threshold value of zero to the Cisco CSG2 with a 0x3 flag. The 0x3 flag indicates that the value is valid.

- CSCtq83301

High CPU GTP management process prevents create PDP context requests from being dropped.

This condition occurs when several create PDP context requests are pending and a subsequent retry request from the same users occur. Typically, this condition might occur when the GGSN is configured for RADIUS authentication and responses to the RADIUS requests are pending, delayed, or have received no response.

- CSCtr30034
The Cisco GGSN might erroneously detect a serving GPRS support node (SGSN) path restart, even though there is no Recovery information element (IE) change in any of the PDP requests.
This condition might occur when a subscriber is trying to connect from one SGSN and immediately moves to another SGSN and sends a create PDP context request.
- CSCtr30035
The Cisco GGSN might reload at PC gprs_red_unpack_pdpcb(). This condition might be triggered by the availability of secondary PDP sessions on the GGSN.
- CSCtr53655
Under stress conditions, PDP sessions become stuck in a “Pending” state and they are unable to connect. This condition occurs with an enhanced GGSN (eGGSN) service-aware implementation.

Cisco SAMI Resolved Caveats

There are no Cisco SAMI caveats newly resolved with Cisco IOS Release 12.4(15)XQ8.

- CSCtn95286
At high traffic loads, the Cisco SAMI might reload as a result of a failure of power convertor 0x5.
%OIR-SP-6-PWRFAILURE: Module 2 is being disabled due to power convertor failure 0x5
%C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (FRU-power failed)

Caveats - Cisco IOS Release 12.4(15)XQ7

This section contains the following types of caveats that pertain to Cisco IOS Release 12.4(15)XQ7:

- [Open Caveats, page 18](#)
- [Resolved Caveats, page 19](#)

Open Caveats



Note

Open caveats for a release also apply to the prior releases.

The following sections document possible unexpected behavior and describe only severity 1 and 2 caveats, and select severity 3 caveats.

- [Cisco GGSN Open Caveats, page 18](#)
- [Cisco SAMI Open Caveats, page 18](#)
- [Miscellaneous Open Caveats, page 19](#)

Cisco GGSN Open Caveats

There are no known Cisco GGSN caveats open in Cisco IOS Release 12.4(15)XQ7.

Cisco SAMI Open Caveats

There are no known Cisco SAMI caveats open with Cisco IOS Release 12.4(15)XQ7.

Miscellaneous Open Caveats

There are no known miscellaneous software caveats open in Cisco IOS Release 12.4(15)XQ7.

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(15)XQ7. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- [Cisco GGSN Resolved Caveats, page 19](#)
- [Cisco SAMI Resolved Caveats, page 20](#)
- [Miscellaneous Resolved Caveats, page 21](#)

Cisco GGSN Resolved Caveats

This section lists the Cisco GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(15)XQ7.

- CSCsx18115

Service-aware PDP contexts might remain in memory after a call is released. This condition might occur under high stress condition (>99% CPU) for several hours for service-aware PDPs.

- CSCta15966

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

- CSCtd10712

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

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

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

Cisco has released free software updates that address these vulnerabilities.

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

- CSCth03022

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities.

Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

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

- CSCth69364
Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.
Cisco has released free software updates that address this vulnerability.
This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml>.
- CSCtj52610
The synchronization of PDPs on the GGSN fails, which leads to a high CPU.
- CSCtj61508
The connection to the quota server is flapping on the Cisco CSG2 when implemented in an eGGSN solution. This condition occurs when the Cisco GGSN is running Cisco IOS Release 12.4(15)XQ5 and later.
- CSCtj72927
The A-flag is not set in Cisco GGSN IPv6 router advertisements.
This condition occurs when the virtual-template on the GGSN is configured with the **ipv6 nd prefix default infinite infinite off-link** command.
- CSCtj99555
The Cisco GGSN crashes when an snmpwalk is made over cGtpPathStatisticsTable. This condition occurs when paths are created and removed (PDPs are created and deleted, or charging gateways are configured and unconfigured) during the snmpwalk.
This issue is seen in Cisco GGSN 12.4(24)YE1 or prior releases when an snmpwalk is made over cGtpPathStatisticsTable.
- CSCtk54730
GTPv0 PDPs are hanging. This condition occurs when an SGSN sends a GTPv0 create request for an already existing PDP associated with a virtual APN.
- CSCtk76072
The Cisco GGSN reloads and the PC of the reload points to serv_tmr_service_chain routine.
This condition occurs under rare circumstances while the Cisco GGSN is experiencing high traffic conditions.
- CSCtn14284
An AAA access-request returns with an internal error, and on the Cisco GGSN the following unconditional bug information is printed: "AAA had an unexpected return."
This condition occurs when an access-request is sent to the AAA server during periods of stress conditions on the client process and a failure to build the RADIUS packet occurs.
- CSCtn42411
The downstream traffic volume in GGSN CDRs stays at 0. This condition occurs when an MS has sent or received more than 4 GB of data.

Cisco SAMI Resolved Caveats

There are no Cisco SAMI caveats resolved with Cisco IOS Release 12.4(15)XQ7.

Miscellaneous Resolved Caveats

This section lists the miscellaneous caveats that are resolved in Cisco IOS Release 12.4(15)XQ7.

- CSCtk13992

In an enhanced GGSN (eGGSN) deployment with Gx-enabled users, the Cisco CSG2 could stop processing certain requests, such as Gx (Diameter requests), causing subscriber outages. The CSG2 could also fail to log in remotely over SSH, generating the following message:

SAMI 4/3: %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0)

- CSCtl48268

The Cisco SAMI application could crash as a result of a memory corruption or accessing an invalid address. The logs from the crashinfo show that the PCRF sent Diameter protocol errors.

Caveats - Cisco IOS Release 12.4(15)XQ6

This section contains the following types of caveats that pertain to Cisco IOS Release 12.4(15)XQ6:

- [Open Caveats, page 21](#)
- [Resolved Caveats, page 22](#)

Open Caveats



Note

Open caveats for a release also apply to the prior releases.

The following sections document possible unexpected behavior and describe only severity 1 and 2 caveats, and select severity 3 caveats.

- [Cisco GGSN Open Caveats, page 21](#)
- [Miscellaneous Open Caveats, page 21](#)

Cisco GGSN Open Caveats

There are no known Cisco GGSN caveats open for Cisco IOS Release 12.4(15)XQ6.

Cisco SAMI Open Caveats

There are no known Cisco SAMI caveats open for Cisco IOS Release 12.4(15)XQ6.

Miscellaneous Open Caveats

There are no known miscellaneous software caveats open for Cisco IOS Release 12.4(15)XQ6.

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(15)XQ6. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- [Cisco GGSN Resolved Caveats, page 22](#)
- [Cisco SAMI Resolved Caveats, page 23](#)
- [Miscellaneous Resolved Caveats, page 24](#)

Cisco GGSN Resolved Caveats

This section lists the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(15)XQ6

- CSCtb09757
The Cisco GGSN encounters a CPU spike on the SNMP-ENGINE process when an snmpwalk is made over ciscoGprsAccPtMIB. This condition occurs when querying ciscoGprsAccPtMIB when there are existing PDPs.
- CSCte44460
During periods of high data rates, the “GPRS:Managed Chunk malloc failed to enqueue” message floods the screen. This condition occurs when the Cisco GGSN processor is at the maximum number of PDP contexts and the data rate is exceeding 120 kpps.
- CSCte57518
The GGSN processor receives a fatal error when the **show ip iscsi session detail** command is executed. This condition occurs when two iSCSI sessions have been created, and the **show ip iscsi** command issued for both sessions.
- CSCte99167
The counters that display when framed routes are inserted are not incremented in the **show gprs gtp statistics** command output. This condition occurs when framed routes are inserted for network-behind mobile.
- CSCtg07230
The PDP contexts on the active GGSN are not synchronized to the standby GGSN even when the redundancy state displays as ACTIVE and STANDBY HOT pair.
This condition was seen only once, and only after repeated reloads were reported due to network issues.
- CSCtg64836
When the TCP connection between the Cisco GGSN and the charging gateway goes down due to network issues, the GGSN writes a syslog that indicates the receipt of “CORRUPTED BYTES” from the charging gateway. This syslog should be seen only when the GGSN receives unexpected data in the TCP stream and not for the error conditions mentioned above.
This condition occurs whenever the TCP connection between the GGSN and charging gateway goes down because of network issues.
- CSCth25554
The Cisco GGSN attempts to access a freed socket pointer for the TCP connection between the charging gateway and the GGSN when the TCP read attempt fails. This incorrect access of a freed pointer might cause memory corruption issues.
The condition occurs when freed memory access is done when the GGSN attempts to read from the TCP socket and the read fails due to incorrect data length.

- CSCth28649
I/O memory leak occurs on the GGSN when create request with different restart values is received on the same signaling path from the SGSN.
This condition occurs when the create request is received with a different restart counter on the same signaling path.
- CSCti81681
The Cisco GGSN might crash when with the following sequence of configuration steps:
 1. Configure multiple class-map.
 2. Configure the policy-map command with the class-map configured in 1. Associate actions with this class-map in the policy-map.
 3. Configure the policy-map under APN as service-policy.
 4. Un-configure the service-policy under APN.
 5. Delete all class-maps under the policy-map and reconfigure them.
 6. Configure the service-policy again under the APN.
 The crash occurs after Step 6.
- CSCti93144
When an access control list (ACL) with Layer 4 (L4) information is configured to permit packets with specific L4 information (for example, port range, etc.), the non-initial fragments are dropped. This behavior is dependent on the complete ACL lines. Equivalent undesired behavior might be observed when the ACL is for deny.
This condition occurs with an ACL with L4 information configured under an APN, and incoming packets (upstream or downstream) have IP fragmentation. With upstream packets, this problem occurs when the inner packets are fragments and the out (GTP) packets are complete.
- CSCsw86589
PDPs remain in a pending state for create requests if the IP address pool has exhausted its available IP addresses. This condition is seen when the create PDP context request is assigned an IP address via downloadable pool name support on an APN (**ip-address-radius-client** access-point configuration command) and the IP address pool has exhausted its available addresses.

Cisco SAMI Resolved Caveats

This section lists the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(15)XQ6.

- CSCtg09217
One or more processors in a SAMI reported a data path health-monitoring failure to an IXP2800 on the SAMI and the SAMI reloaded. A message similar to “PLATFORM-1-DP_HM_FAIL: Failed to receive response from IXP1” displayed.
If a standby Cisco GGSN was configured, the standby GGSN took over as the active GGSN.

Miscellaneous Resolved Caveats

This section lists the miscellaneous caveats that are resolved in Cisco IOS Release 12.4(15)XQ6.

- CSCso89298

Description: Reconfiguring service-policy under an APN does not work as designed. If the service-policy is removed and reattached, it might stop working.

Workaround: There is currently no known workaround.

- CSCsw25408

The Cisco GGSN policy map configuration is not taking effect when conform, exceed, and violate actions are configured using the **police rate pdp** command in policy map configuration mode. This condition occurs only when the policy map is configured in the policy map configuration mode.

- CSCsw68626

When a configured server name is removed from an AAA server group using the **no server name** command, the router crashes.

- CSCsy55362

Console might hang when the TACACS+ server is being used as an AAA server and the single connection option is configured.

- CSCte69879

The **ip radius source-interface** command for Accounting On/Off does not work if it is configured under an AAA group.

- CSCtf68469

The aggregated U-routes present in the routing table are deleted, even when valid PDP contexts are present on a route. This condition is seen only when there are more than 65535 PDP contexts corresponding to the same U-route (when single route aggregation is used for IP pools that have more than 65535 IP addresses).

- CSCtf71296

The iSCSI state in the **show ip iscsi session** command output displays as “Free” when the connection to the iSCSI target is brought down asynchronously.

- CSCth38615

The charging gateway status on the TCOPs goes out of sync when one of the TCOPs receives a corrupted byte stream on the TCP connection between the GGSN and the charging gateway. While the charging gateway status is UNDEFINED in the TCOP that received the corrupted byte stream, the other TCOPs still show its status as ACTIVE.

This condition is seen if one or more TCOPs receives a corrupted byte stream from the charging gateway and closes the TCP connection.

Caveats - Cisco IOS Release 12.4(15)XQ5

This section contains the following types of caveats that pertain to Cisco IOS Release 12.4(15)XQ5:

- [Open Caveats, page 25](#)
- [Resolved Caveats, page 26](#)

Open Caveats

**Note**

Open caveats for a release also apply to the prior releases.

The following sections document possible unexpected behavior and describe only severity 1 and 2 caveats, and select severity 3 caveats.

- [Cisco GGSN Open Caveats, page 25](#)
- [Miscellaneous Open Caveats, page 25](#)

Cisco GGSN Open Caveats

This section lists the Cisco GGSN-specific caveat that are open in Cisco IOS Release 12.4(15)XQ5.

- CSCsw86589

PDPs remain in a pending state for creates if the IP address pool has exhausted its available IP addresses. This condition is seen when the create PDP context request is assigned an IP address via downloadable pool name support on an APN (**ip-address-radius-client** access-point configuration command) and the IP address pool has exhausted its available addresses.

Workaround: Ensure that the IP addresses are available for the pool name downloaded via the RADIUS Access-Accept message.

- CSCtd61508

The Cisco GGSN increments interim accounting counters in the standby node and the **show gprs gtp pdp-context tid** command output on the standby node includes the “next due at” counter when it should not.

Workaround: There is currently no known workaround.

- CSCte44460

During periods of high data rates, the “GPRS:Managed Chunk malloc failed to enqueue” message floods the screen. This condition occurs when the Cisco GGSN processor is at the maximum number of PDP contexts and the data rate is exceeding 120 kpps.

Workaround: There is currently no known workaround. When the data rate or the number of PDP contexts are reduced, the message subsides.

Miscellaneous Open Caveats

The following miscellaneous software caveat is open for Cisco IOS Release 12.4(15)XQ5.

- CSCtf68469

The aggregated U-routes present in the routing table are deleted, even when valid PDP contexts are present on a route. This condition is seen only when there are more than 65535 PDP contexts corresponding to the same U-route (when single route aggregation is used for IP pools that have more than 65535 IP addresses).

Workaround: Configure IP pools with less than 65535 entries in one pool and configure different route aggregation for each pool

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(15)XQ5. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- [Cisco GGSN Resolved Caveats, page 26](#)
- [Cisco SAMI Resolved Caveats, page 27](#)
- [Miscellaneous Resolved Caveats, page 27](#)

Cisco GGSN Resolved Caveats

This section lists the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(15)XQ5.

- CSCsx78006

When the charging path protocol is TCP, data transfer record (DTR) transmission to charging gateway (CG) fails even though the link between the GGSN and the CG is restored. This condition is initially triggered by communication loss between the GGSN and the CG, which causes the GGSN to buffer multiple (up to 20) pending DTRs. Once this condition occurs, the retransmitted DTRs do not include the GTP' header; therefore, they are discarded by the CG. This again results in GGSN bringing down the TCP link because of lack of acknowledgement by charging gateway. A subsequent node alive message from CG reestablishes the link, but the error condition persists and the same sequence repeats.
- CSCsz42882

With iSCSI link flaps, stale file systems remain in the system. Once the stale file descriptors reach the max supported limit, iSCSI link doesn't come up as new filesystem can not be created. GGSN box would need a reload to clear the stale file systems.
- CSCte20052

When a create PDP context request message is received after an SGSN reload, an infinite loop occurs in the "GTP Management" process.
- CSCte51938

GTP and access-point statistics are not synchronized to the standby GGSN. This issue is seen on the standby GGSN when the **show gprs gtp statistics** command and the **show gprs access-point statistics** command are executed.
- CSCte65329

When using TCP as the path protocol for the charging interface, the Cisco GGSN CPU is sometimes seen at 100% utilization with the GTP I/O process occupying the bulk of the CPU. Because of this, GTP transfer failures occur on the charging path and CDRs start accumulating (buffering) on the system. The Cisco GGSN does not recover from this condition, which can eventually cause system memory depletion and related symptoms due to continuous buffering of CDRs.

This condition is seen when the charging gateway sends corrupted or invalidbyte streams towards the GGSN on the TCP socket established between the GGSN and the charging gateway. The corrupted byte stream results in system error logs such as "LFN bit in CHRG msg should be set" since the charging gateway sends packets with 20-byte headers even though the charging path and GGSN are configured to process 6-byte headers. Eventually, the corrupted byte stream causes the GTP I/O process in the GGSN to take up the bulk of the CPU causing the symptoms listed above.
- CSCtf06284

After the Cisco GGSN transitions from standby to active, the SNMP counters for the `cgprsAccPtStatisticsEntry` and `cGgsnStatistics` objects are incorrect.

- CSCtf68451

In Cisco IOS Release 12.4(15)XQ3, the Cisco GGSN default behavior of dropping T-PDUs without a sequence number (s=0) was changed to allow T-PDUs without a sequence number. This new behavior applies to when the Cisco GGSN receives a T-PDU without a sequence number (s=0) in the GTPv1 header, and the reorder-required in the PDP is set to TRUE.

The **[no] gprs gtp tpdu reorder-required sequence receive mandatory** global configuration command has been added to enable the configuration of the Cisco GGSN behavior:

For more information, see the “[New Implementations and Behavior Changes in Cisco IOS Release 12.4\(15\)XQ5](#)” section on page 10.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI software caveats with Cisco IOS Release 12.4(15)XQ5.

Miscellaneous Resolved Caveats

This section lists the miscellaneous caveats that are resolved in Cisco IOS Release 12.4(15)XQ5.

- CSCsy09250

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

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

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

- CSCsz07615

When the **reload** command is issued, it takes some time to bring down the system, and during the process, it takes an unusually long amount of time for the redundancy protocols to notify peers. This condition causes some timing issues, and only occurs with redundancy protocols such as Hot Standby Router Protocol (HSRP).

- CSCsz75186

A device running Cisco IOS might display the following message and reload:

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = IP Input.
```

Caveats - Cisco IOS Release 12.4(15)XQ4

This section contains the following types of caveats that pertain to Cisco IOS Release 12.4(15)XQ4:

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

Open Caveats



Note

Open caveats for a release also apply to the prior releases.

The following sections document possible unexpected behavior and describe only severity 1 and 2 caveats, and select severity 3 caveats.

- [Cisco GGSN Open Caveats, page 28](#)
- [Cisco SAMI Open Caveats, page 28](#)
- [Miscellaneous Open Caveats, page 28](#)

Cisco GGSN Open Caveats

This section lists the Cisco GGSN-specific caveat that is open in Cisco IOS Release 12.4(15)XQ4.

- CSCsy34950

After a reboot, traffic from the user data plane does not leave the Cisco GGSN any longer because no Address Resolution Protocol (ARP) entry exists on the GGSN for the default route (next hop, Cisco CSG2).

This condition occurs only when the `redirect all ip` command is configured when running new CEF code. The new CEF code introduces neighbor resolution optimization (enabled by default) which has issues with ARP packet handling.

Workaround: Disable the optimization by using the `no ip cef optimize neighbor resolution` command on the Cisco GGSN.

Cisco SAMI Open Caveats

There are no Cisco SAMI software caveats open with Cisco IOS Release 12.4(15)XQ4.

Miscellaneous Open Caveats

There are no miscellaneous software caveats open with Cisco IOS Release 12.4(15)XQ4.

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(15)XQ4. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- [Cisco GGSN Resolved Caveats, page 28](#)
- [Cisco SAMI Resolved Caveats, page 29](#)
- [Miscellaneous Resolved Caveats, page 29](#)

Cisco GGSN Resolved Caveats

This section lists the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(15)XQ4.

- CSCsr19491

Description: A charging collection time out occurs for every path echo interval time when it should only occur when a collection timeout occurs.

- CSCsx19498

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

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

- CSCta34630
Description: When a create PDP context request is received that has an IP source address that is different from the SGSN address for signalling and data, the signalling message received on the path statistics does not increment correctly. This condition occurs only when the IP source address is different from the SGSN address for signalling and data.
- CSCta53732
Description: The Cisco GGSN might end up with stale PDP contexts when different GTP version create PDP context requests are received from different SGSNs (signaling and data different) with different Restart values.
- CSCtb49987
Description: The number of IP addresses allocated does not match in the active and standby GGSN. The numbers on the active GGSN are correct.
- CSCtb77302
Description: The Cisco GGSN sends 3GPP TS 32.215 Release 7 charging info, radio access technology (RAT), User Location, and MS TimeZone, even when the configured charging configuration is earlier than Release 7.
- CSCtb77620
Description: Due to missing 3GPP specifications, the Cisco GGSN might mix two PDP sessions into one when one of the following scenarios occurs:
 - With an Update PDP Context request for a session with Tunnel Endpoint Identifier (TEID) 0x0000yyyy assigned in GTP version 1 (GTPv1) communication between the GGSN and SGSN, in the handover scenario in which GTPv1 exists between the source SGSN and GGSN and GTPv1 between the target SGSN and GGSN.
 - With an Update PDP Context request for a session which was assigned in GTPv0 communication between the GGSN and SGSN with a flow label 0xyyyy, in the handover scenario in which a handover is made to GTPv1 between the target SGSN and GGSN while both source and target SGSNs talk with each other with GTPv1.
- CSCtc07857
Description: Under rare conditions, a fatal error may occur with GTP parsing of PPP.
- CSCtc34938
Description: Some Cisco GGSN processors on the standby SAMI reload with an “RF induced self-reload” syslog message.

Cisco SAMI Resolved Caveats

There are no new Cisco SAMI software caveats resolved with Cisco IOS Release 12.4(15)XQ4.

Miscellaneous Resolved Caveats

This section lists the miscellaneous caveats that are resolved in Cisco IOS Release 12.4(15)XQ4.

- CSCta49840
Description: In a virtual private dialup network (VPDN)/Layer 2 Tunneling Protocol (L2TP) configuration, the Cisco GGSN might encounter a fatal error. This error might occur in very rare conditions when the physical connectivity on interface to the L2TP network server (LNS) is lost while there are active sessions and traffic.

- CSCtb93855
The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.
Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device if H.323 is not required.
This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20100324-h323.shtml>.
- CSCsv30595
Description: The Open Shortest Path First (OSPF) process might receive a fatal error when the router receives invalid OSPF messages.
- CSCsv34656
Description: A particular malformed OSPF message might cause the device to fail or operate unpredictably. This condition is seen when the OSPF receives a malformed OSPF message and the possible effects include the following:
 - The router might receive a fatal error.
 - Routing loops might form in the network.
 - OSPF might control the CPU and drop adjacencies.
 - The **show ip ospf database net** command output displays unwanted lines.
- CSCsw78939
Description: No new sessions can come up after using VPDN a few days.
- CSCsy15227
Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent web page.
There are no workarounds that mitigate this vulnerability.
This advisory is posted at the following link:
<http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml>
- CSCsz38104
The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml>.

Caveats - Cisco IOS Release 12.4(15)XQ3

This section contains the following types of caveats that pertain to Cisco IOS Release 12.4(15)XQ3.

Open Caveats

**Note**

Open caveats for a release also apply to the prior releases.

The following sections document possible unexpected behavior and describe only severity 1 and 2 caveats, and select severity 3 caveats.

- [Cisco GGSN Open Caveats, page 31](#)
- [Cisco SAMI Open Caveats, page 31](#)
- [Miscellaneous Open Caveats, page 31](#)

Cisco GGSN Open Caveats

This section lists the Cisco GGSN-specific caveats that are open in Cisco IOS Release 12.4(15)XQ3.

- CSCsr19491

Description: A charging collection time out occurs for every path echo interval time when it should only occur when a collection timeout occurs.

Workaround: Disable the echo between the GGSN and the charging gateway.

- CSCsy34950

After a reboot, traffic from the user data plane does not leave the Cisco GGSN any longer because no Address Resolution Protocol (ARP) entry exists on the GGSN for the default route (next hop, Cisco CSG2).

This condition occurs only when the redirect all ip command is configured when running new CEF code. The new CEF code introduces neighbor resolution optimization (enabled by default) which has issues with ARP packet handling.

Workaround: Disable the optimization by using the **no ip cef optimize neighbor resolution** command on the Cisco GGSN.

Cisco SAMI Open Caveats

There are no Cisco SAMI caveats open for Cisco IOS Release 12.4(15)XQ3.

Miscellaneous Open Caveats

The following miscellaneous software caveat is open for Cisco IOS Release 12.4(15)XQ3.

- CSCta49840

Description: In a VPDN/L2TP configuration, the Cisco GGSN might encounter a fatal error. This error might occur in very rare conditions when the physical connectivity on interface to the LNS is lost while there are active sessions and traffic.

Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(15)XQ3. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- [Cisco GGSN Resolved Caveats, page 32](#)
- [Cisco SAMI Resolved Caveats, page 35](#)
- [Miscellaneous Resolved Caveats, page 35](#)

Cisco GGSN Resolved Caveats

This section lists the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(15)XQ3.

- CSCsq92712

Description: A Cisco SAMI processor might reload when iSCSI-related commands are reconfigured (or unconfigured and configured). This condition can occur when a large number of pending CDRs (over one million) are being written to the iSCSI storage device under extremely high signaling and network traffic, and CPU and memory utilization is over 90% and 95% respectively.
- CSCsv46234

Description: When a PDP session with an extended profile is established to an APN that has CAC and a bandwidth pool configured, if the bandwidth pool remaining is less than what is consumed by the session, a COA with the same QoS profile as the already established PDP session, or a COA to downgraded QoS profile fails.

For example, assume the available bandwidth pool is 400000, and after the PDP session is established it consumes 300000, a COA with a QoS profile that is the same as the profile of the established PDP session, or a downgraded QoS profile via a COA will fail.
- CSCsv62355

Description: When unconfiguring a Proxy Call Session Control Function (P-CSCF) group, the P-CSCF group appears to still be in use, even though the PDP contexts and APNs have been removed.
- CSCsv73505

Description: Prepaid quota usage is not reported to the Online Charging Server (OCS), and as a result, reauthorization is not occurring when QoS Change is the armed trigger from the OCS. This condition is seen when the QoS Change happens via Change of Authorization (CoA) message from the Policy and Charging Rules Function (PCRF).
- CSCsv94056

Description: For a GTPv1 service aware prepaid PDP context with a service that has radio access technology (RAT) as the armed trigger, a GTPv1-to-GTPv0 handoff, and subsequent GTPv0 update PDP context requests without any RAT change, causes the Cisco GGSN to reauthorize the service and close the service record with the change condition as RAT change even though RAT has not changed.
- CSCsw78447

Description: Once a disk full condition is reached on an iSCSI device, the Cisco GGSN fails to write more CDRs to the iSCSI device when more space is created on the device. This condition rarely occurs, and only when no auto-retrieval is configured on the GGSN.

- CSCsw86972
Description: A traceback related to the “Process=GPRS Charging Transfer” is printed on the console while CDRs are sent to an iSCSI target. This traceback is seen once for every processor reload, and when the CDRs are transferred for the first time to the iSCSI target.
- CSCsx02916
Description: When one of the Cisco SAMI PowerPCs (PPCs) is overloaded with traffic, in some circumstances, the other PPCs on the same daughter card will generate SAMI health monitoring errors and might restart.
- CSCsx05788
Description: The Cisco GGSN might fail to send an accounting stop message to the AAA server on a PPP-Regeneration enabled APN when the **network-behind-MS** command and the **security verify source** command are both configured on the APN.
- CSCsx07725
Description: A CoA with extended QoS profile for the PDP context might cause spurious memory access when:
 1. UMTS QoS is configured on the GGSN
 2. Service aware prepaid user PDP and QoS change is armed by the DCCA.
- CSCsx11167
Description: The Cisco GGSN should send the Gn interface address in billing records when the source interface is configured as the charging source.
- CSCsx15322
Description: The QoS value is different in a captured GTP control packet than in the debug log.
 Debug log example:


```
Maximum bit rate for uplink:504kbps
Maximum bit rate for downlink:1160kbps
```

 GTP control packet example:


```
Maximum bit rate for uplink : 2048 kbps
Maximum bit rate for downlink : 7296 kbps
```
- CSCsx21938
Description: The Cisco GGSN sends the MSISDN as the username in the Start Accounting message, whereas for the same session, the LNS shows the actual username itself. The Cisco GGSN appears to be forwarding the MSISDN value during the Create PDP Context process to the LNS.
- CSCsx25641
Description: The Cisco GGSN connection to a charging gateway might fail during initialization or bootup, and the Cisco GGSN will not attempt to reconnect without user intervention. This condition might occur when the path is set to UDP and charging echo is disabled.
- CSCsx35449
Description: The Cisco GGSN rejects Create PDP Context requests when more than 16Mb GBR is requested. This condition occurs only when the requested GBR is more than the supported bit rate for each PDP.

- CSCsx43681
Description: On a Cisco GGSN, if a CCA response is received with 4016 as the result code, the DCCA CC-session is kept in a PENDING_U state indefinitely. This condition occurs only when the previous CCR update receives a CCA with a 4016 result code.
- CSCsx55090
Description: The Cisco GGSN appends some extra bytes when closing files in iSCSI. This condition occurs only when the file to which the CDR is being written has to be closed because the file size has been reached.
- CSCsx71970
Description: The Cisco GGSN reloads when a restart count changes on a secondary PDP context. When the GGSN receives a secondary create PDP context request with a different restart count, it deletes all existing PDP contexts associated with the path, and creates a new PDP context. The GGSN reloads when there is an attempt to clear the new PDP context using the **clear gprs gtp pdp-context all** command or when the GGSN receives a Delete PDP Context request to clear the PDP context.
- CSCsx73172
Description: Changing the Cisco GGSN charging configuration while billing records are being sent causes the GGSN to receive a fatal error. This condition is observed while billing records are being sent to an active Billing Mediation Agent (BMA) and the GGSN charging configuration is being changed at the same time.
- CSCsx97474
Description: Memory leaks might occur at the process level when charging is enabled on the Cisco GGSN and the system is under heavy stress continuously transferring charging records and DTRs to the charging gateways. The extent of the leaks is minor and is not expected to affect the system performance.
- CSCsy70508
Description: The standby GGSN has a less number of sessions than the active GGSN when DHCP addressing is used. When PDP contexts are created and deleted, the standby GGSN is erroneously deletes some active sessions. This condition results in less number of active sessions on standby GGSN than on the active GGSN.
- CSCsz33490
Description: When a QoS update occurs for a GTPv0 service aware postpaid PDP with a QoS trigger enabled, the categories are not affected. This condition occurs only with postpaid PDPs with the GGSN acting as the quota server with DCCA disabled.
- CSCsz83906
Description: Because of an invalid %s specified in a printf statement, a traceback occurs while printing a CLI error message. This condition was observed when changing the GPRS iSCSI record format from GTP to ASN.1.
- CSCsz85678
Description: The Cisco GGSN (running on a Cisco SAMI with the 2 GB memory option) does not permit the creation of more than 128000 IP PDPs.
- CSCta02056
Description: A PPP session setup failed because of a missing sequence number in the T-PDU packet.

Cisco SAMI Resolved Caveats

This section lists the Cisco SAMI software caveats that are resolved for Cisco IOS Release 12.4(15)XQ3.

- CSCsw83383

Description: In certain cases, crashinfo might not be written when a Cisco SAMI processor suddenly reloads. This occurs under a very rare condition where the CPU is higher than 90% and memory utilization is above 95%.

- CSCsx58009

Description: The Cisco SAMI PPCs receive a fatal error due to a SegV exception at the L2TP process. The condition occurs approximately 17 seconds after receiving the last L2TP hello packet when L2TP communication between LAC and LNS is down more than 180 seconds.

- CSCsx68809

Description: Occasionally, when Cisco SAMI PPCs are reloaded, they become unresponsive and are unable to bootup. A session to the PPCs cannot be established and the **show sami processors** command issued from the LCP (PPC0) console displays the status of the PPCs as “ROMMON INITIALIZING (0x00000800).”

Miscellaneous Resolved Caveats

This section lists the miscellaneous caveats that are resolved in Cisco IOS Release 12.4(15)XQ3.

- CSCso90058

Description: RedZone corruption causes device reload. SFC crashes with Red Zone memory corruption. This problem is seen when processing an Auto-RP packet and NAT is enabled.

- CSCsq24002

Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at

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

- CSCsr74835

Description: An overflow of destination buffer might occur because of unspecified bounding length.

- CSCsv73509

Description: When **no aaa new-model** is configured, authentication occurs through the local even when TACACS is configured. This happens for EXEC users under the VTY configuration.

This condition is observed when you configure **no aaa new-model**, configure **login local** under **line vty 0 4**, and configure **login tacacs** under **line vty 0 4**.

- CSCsx97093

Description: When trying to parse a callback string attribute in an ACCESS-ACCEPT that has no callback value, RADIUS/DECODE fails:

```
*Feb 24 16:04:22.252: RADIUS: Received from id 1645/68 10.48.88.121:19645,
Access-Accept, len 52
*Feb 24 16:04:22.252: RADIUS:  authenticator 49 7C 52 33 F8 BF 21 49 - 6C EF EC 2C 6D
09 92 BD
*Feb 24 16:04:22.252: RADIUS:  Vendor, Cisco          [26] 32
*Feb 24 16:04:22.252: RADIUS:  Cisco AVpair          [1] 26
"lcp:callback-dialstring="
*Feb 24 16:04:22.252: RADIUS(00000000): Received from id 1645/68
*Feb 24 16:04:22.252: RADIUS/DECODE: convert VSA string; FAIL
*Feb 24 16:04:22.252: RADIUS/DECODE: cisco VSA type 1; FAIL
*Feb 24 16:04:22.252: RADIUS/DECODE: VSA; FAIL
*Feb 24 16:04:22.252: RADIUS/DECODE: decoder; FAIL
*Feb 24 16:04:22.252: RADIUS/DECODE: attribute Vendor-Specific; FAIL
*Feb 24 16:04:22.252: RADIUS/DECODE: parse response op decode; FAIL
```

Any of the following callbacks fail parsing when configured with NULL value:

```
"arap:callback-dialstring="
"slip:callback-dialstring="
"shell:callback-dialstring="
"lcp:callback-dialstring="
```

Caveats - Cisco IOS Release 12.4(15)XQ2

This section contains the following types of caveats that pertain to Cisco IOS Release 12.4(15)XQ2.

Open Caveats



Note

Open caveats for a release also apply to the prior releases.

The following sections document possible unexpected behavior and describe only severity 1 and 2 caveats and select severity 3 caveats.

- [Cisco GGSN Open Caveats, page 36](#)
- [Cisco SAMI Open Caveats, page 37](#)
- [Miscellaneous Caveats, page 38](#)

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(15)XQ2.

- CSCsq92712

Description: A SAMI processor might reload when iSCSI-related commands are reconfigured, or unconfigured and configured. This condition can occur when a huge number of pending CDRS (over one million) are being written to the storage device under extremely high signaling and network traffic with CPU and memory utilization of over 90% and 95% respectively.

Workaround: Avoid reconfiguring iSCSI-related commands in extremely high CPU and memory bound conditions.

- CSCsv46234

Description: When a PDP session with an extended profile is established to an APN that has CAC and a bandwidth pool configured, if the bandwidth pool remaining is less than what is consumed by the session, a COA with the same QoS profile as the already established PDP session, or a COA to downgraded QoS profile fails.

For example, assume the available bandwidth pool is 400000, and after the PDP session is established it consumes 300000, a COA with a QoS profile that is the same as the profile of the established PDP session, or a downgraded QoS profile via a COA will fail.

Workaround: There is currently no known workaround.

- CSCsw78447

Description: Once a disk full condition is reached on an iSCSI device, the GGSN fails to write more CDRs to the iSCSI device when more space is created on the device. This condition rarely occurs, and only when no auto-retrieval is configured on the GGSN.

Workaround: Avoid disk full conditions by periodically monitoring and freeing space on the storage device. If the disk reaches the condition, reload the processor to resume writing CDRs to the external device.

- CSCsy34950

After a reboot, traffic from the user data plane does not leave the Cisco GGSN any longer because no Address Resolution Protocol (ARP) entry exists on the GGSN for the default route (next hop, Cisco CSG2).

This condition occurs only when the redirect all ip command is configured when running new CEF code. The new CEF code introduces neighbor resolution optimization (enabled by default) which has issues with ARP packet handling.

Workaround: Disable the optimization by using the **no ip cef optimize neighbor resolution** command on the Cisco GGSN.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI software caveats that are open for Cisco IOS Release 12.4(15)XQ2.

- CSCso02063

Description: Increasing the MTU configured on the GigabitEthernet0/0 interface of the SAMI from the default value of 1500 bytes might cause some packets to be dropped in the ingress direction.

Packet drops might be seen only when the MTU configured on the GigabitEthernet0/0 interface of the SAMI is greater than 4067 bytes and drops are only seen for fragmented packets of certain sizes.

Workaround: Ensure that the MTU of the GigabitEthernet 0/0 interface of the SAMI is configured to be less than or equal to 4067.

- CSCso77755

Description: A SAMI processor might reload again during bootup or if the user executes a file check operation to the bootflash. This behavior occurs under very rare conditions where the flash card has a corrupted file spanning multiple sectors.

Workaround: Copy and clear any crashinfo files from the processor bootflash. Also, avoid running any file check on the bootflash. To recover from this condition, establish a session with processor 0 of the SAMI card (username:admin, password:admin) and issue the **erase ppc-flash ppc-number** command. This command takes a few minutes. After the command is completed, issue the **reload sami processor ppc-num** command.

Miscellaneous Caveats

This section lists the miscellaneous caveat that is open for Cisco IOS Release 12.4(15)XQ2.

- CSCta49840

Description: GGSN may run into a fatal error in VPDN/L2TP configurations. This condition may occur in rare race conditions when physical connectivity on interface to LNS is lost while there are active sessions and traffic.

Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(15)XQ2. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- [Cisco GGSN Resolved Caveats, page 38](#)
- [Cisco SAMI Resolved Caveats, page 42](#)
- [Miscellaneous Resolved Caveats, page 42](#)

Cisco GGSN Resolved Caveats

This section lists the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(15)XQ2.

- CSCir00863

Description: An IPv6 local pool prefix of more than 64-bits is allowed by the GGSN when it should not allow a prefix length other than 64 bits to be assigned to MS when addressing is from a local IPv6 pool.

- CSCsg00102

Symptoms: SSLVPN service stops accepting any new SSLVPN connections.1

Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

- CSCsk64158

Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml>.

- CSCsm27071

A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

- The configured feature may stop accepting new connections or sessions.
- The memory of the device may be consumed.
- The device may experience prolonged high CPU utilization.
- The device may reload. Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml>

- CSCsm97220

Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at the following link

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml>

- CSCso04657

Description: SSLVPN service stops accepting any new SSLVPN connections.

A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

- CSCso85294

Description: When a version upgrade occurs, the Signaling msg received (sig_msg_rcvd) counter does not increment in the **show gprs gtp path statistics** output.

- CSCsr11468

Description: On a Cisco GGSN, if the SLB next hop address is set by the SNMP command, a memory issue might occur.

- CSCsq09132

Description: In the GTP message, there is a length field in the message header, as well as individual length fields for each information element (IE). These length fields should be consistent, however, for some reason (the sender sends a wrong message or the packet gets corrupted), the following two possibilities occur.

1. The length indicated in header is more than the cumulative lengths of individual IEs.
2. The length indicated in header is less than the cumulative lengths of individual IEs.

If the first possibility occurs, GGSN tries to parse the stray bytes, but fails. If the second possibility occurs, the GGSN tries to access the memory beyond the bound. This might lead to erroneous behavior.

- CSCsq52596
Description: The cef_drop counter does not increment when certain illegal packets such as source violation PDUs are sent. However, the cef counters update correctly.
- CSCsr29468
Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.
Cisco has released free software updates that address this vulnerability.
Several mitigation strategies are outlined in the workarounds section of this advisory.
This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml>
- CSCsv06714
Description: When the Cisco GGSN receives a Credit Control Answer (CCA) with result code as 5012 for a service, it does not process the CCA correctly, keeps service in waiting for the CCA state, and does not send a reply to the Cisco CSG.
- CSCsv11128
Description: On the Cisco GGSN, if the User Location Info IE is not received in a Create PDP Context Request, the GGSN does not include the USER-LOCATION-INFO AVP when requesting quota for a prepaid service.
- CSCsv36185
Description: The Network Behind Mobile configuration (the **network-behind-mobile** access point configuration command) is not accepted.
- CSCsv46079
Description: When the requested QoS exceeds the available bandwidth, the Cisco GGSN does not negotiate the QoS profile as expected.
- CSCsv36834
Description: The NBM downstream traffic for PPP-Regen is not getting tunneled (VPDN->GTP) switch.

- CSCsv38166

The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>.

- CSCsv56109

Description: When the Cisco GGSN receives an echo request on a TCP charging path, it does not send the echo response back to charging gateway.

- CSCsv59019

Description: The Cisco GGSN is not switching data packets for GTPv0 PPP PDPs. This condition only occurs for GTPv0 PDPs when CEF is enabled.

- CSCsv61645

Description: When sessions are cleared after a failure caused by “%GPRSFLTMG-4-ADDRESS_DUPLICATION_PDPACTIVATIONFAIL,” the Cisco GGSN reloads because of unexpected exceptions.

- CSCsv86234

Description: The GGSN stopped forwarding packets for PDPs configured for network behind mobile feature after a failover.

This issue is seen only for Network behind mobile PDPs after a failover.

- CSCsw19315

Description: In case of PDP with Network Behind Mobile, the downstream traffic to the IP address belonging to subnet behind the MS is not getting CEF switched. This condition occurs with NBM traffic only.

- CSCsw64615

Description: With Cisco IOS 12.4(15)XQ2 or later, the feature functionality to send charging records to iSCSI has been enhanced to send either the GTP or the pure ASN.1 mode. ASN.1 mode writes the charging record from the Call Event Record type onward.

To enable the GGSN to generate pure ASN.1 records, the data record format needs to be configured using the **gprs charging iscsi rec-format asn.1** global configuration command.

The records in this format are generated only when auto-retrieval is disabled on the GGSN, which is the default behavior. This configuration should be used only when charging records are stored only on an iSCSI target (the charging gateway should not be configured in this case).

- CSCsw68085

Description: The Cisco GGSN does not open CDRs when the iSCSI target is configured alone and no charging gateway is configured. This enables an iSCSI target to be configured for storing CDRs when there is not a charging gateway.

- CSCsw78328

Description: When issuing the **clear gprs statistics** command while there are active PDP contexts, might result in subsequent SNMP GETs for the `cgprsAccPtActivePdps` OID to report a value that is too high. For example, if there are currently 100 active PDP contexts when the **clear gprs statistics** command is issued, or later the 100 PDP contexts are disconnected, and even later 50 new ones connect, the `cgprsAccPtActivePdps` will incorrectly show 150 active PDP contexts. The CLI will correctly show only a value of 50.

Cisco SAMI Resolved Caveats

This section lists the Cisco SAMI software caveats that are resolved for Cisco IOS Release 12.4(15)XQ2.

- CSCsq88312

Description: A PPC crashes after the **reload** command is issued after creating and deleting a large number of PDPs. This condition does not occur unless a large number of PDPs are being created and deleted.

Miscellaneous Resolved Caveats

This section lists the miscellaneous caveats that are resolved in Cisco IOS Release 12.4(15)XQ2.

- CSCsI11319

Description: If the Cisco IOS mobile wireless applications want to read or write synchronously, the read or write process might not occur as expected. The application might still write asynchronously.

- CSCsj50892

Description: After configuring **no local ip pool** command to remove a specific IP address of range under multiple IP address of range with one **local address pool**, whole IP address of range is removed. An option to specify IP address of range is not valid.

By configuring **no local ip pool** command.

- CSCso18940

Description: The `snmpwalk ipRouteTable` MIB returns an error and the OID is not increasing. This condition occurs on `snmpwalk ipRouteTable` MIB.

- CSCso47637

Description: After a switchover, the newly active GGSN displays less CDRs on the iSCSI disk.

This condition exists after the following occurs:

- Charging gateway is down, CDRs are written to iSCSI.
- Traffic is stopped, the active GGSN is reloaded, and the standby GGSN becomes active
- The newly active GGSN displays less CDRs on the iSCSI disk

- CSCsu49204

Description: A SAMI processor might reload when sending IMIX traffic at 80k packets per second (pps) across 30k PDPs. The system has 60k IP PDPs with Small Computer Systems Interface over IP (iSCSI) backup storage configuration.

- CSCsv04836

Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml>.

- CSCsw42451

Description: There is a 12byte header and a 4byte trailer which is added by iscsi infra for all the records written by ggsn. The ASN.1 decoder is not able to decode the data written in the iscsi target.

When auto-retrieval is not done through the GGSN application and the records are decoded via an ASN.1 decoder.

Retrieve the CDR's via GGSN application using the auto-retrieval feature. For this configure the following command on the ggsn application.

gprs auto-retrieval

- CSCsw78449

The Cisco GGSN processor spontaneously reloads when unconfiguring the iSCSI commands. This condition occurs with a load of 60,000 PDPs and approximately 3 million closed CDRs in the buffer and the **no ip iscsi target-profile** command is executed.

Caveats - Cisco IOS Release 12.4(15)XQ1

**Note**

Open caveats for a release also apply to the prior releases.

This section contains the following types of caveats that pertain to Cisco IOS Release 12.4(15)XQ1.

Open Caveats

The following sections document possible unexpected behavior and describe only severity 1 and 2 caveats and select severity 3 caveats.

- [Cisco GGSN Open Caveats, page 44](#)
- [Cisco SAMI Open Caveats, page 44](#)
- [Miscellaneous Open Caveats, page 45](#)

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(15)XQ1.

- CSCso24734

Description: During the creation of 8000 IPv6 PDP sessions at the rate of 20 calls per second (CPS), the GGSN processor CPU usage is at 99% when approximately 3000 of the 8000 IPv6 PDPs are established.

Workaround: There is currently no known workaround.

- CSCsy34950

After a reboot, traffic from the user data plane does not leave the Cisco GGSN any longer because no Address Resolution Protocol (ARP) entry exists on the GGSN for the default route (next hop, Cisco CSG2).

This condition occurs only when the `redirect all ip` command is configured when running new CEF code. The new CEF code introduces neighbor resolution optimization (enabled by default) which has issues with ARP packet handling.

Workaround: Disable the optimization by using the `no ip cef optimize neighbor resolution` command on the Cisco GGSN.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI software caveats that are open for Cisco IOS Release 12.4(15)XQ1.

- CSCso02063

Description: Increasing the MTU configured on the GigabitEthernet0/0 interface of the SAMI from the default value of 1500 bytes might cause some packets to be dropped in the ingress direction.

Packet drops might be seen only when the MTU configured on the GigabitEthernet0/0 interface of the SAMI is greater than 4067 bytes and drops are only seen for fragmented packets of certain sizes.

Workaround: Ensure that the MTU of the GigabitEthernet 0/0 interface of the SAMI is configured to be less than or equal to 4067.

- CSCsq44633

Description: Sometimes the LCP fails to automatically reboot when the whole SAMI card is reloaded after changing the PPCs' config registers value by executing the **processor all-ppc config-reg** *config reg value* command from the LCP.

This condition rarely occurs and occurs only when the **processor all-ppc config-reg** command is used from the LCP.

Workaround: Once the LCP fails to autoboot and goes to rommon, manually boot the LCP by typing **boot** command in the rommon.

- CSCsq88670

Description: The PPC **reload** command is disabled when a large number of PDP contexts are created and deleted.

Workaround: Reload the entire SAMI rather than a single PPC.

- CSCsu39672

Description: The SAMI might reload while copying an image to it using the upgrade procedure from the supervisor. This condition occurs only after previously terminating an upgrade procedure in the middle of the procedure, and then immediately performing another upgrade procedure. The LCP crashes while the image is being copied to the SAMI from the supervisor.

Workaround: If running the CSG2 application, upgrade the standby CSG2 first, reload it, and then upgrade the formerly primary CSG2.

If this condition occurs, and the SAMI will not boot due to an incomplete upgrade, reset the card by issuing the **boot eobc** command from the supervisor to reload the SAMI. For the detailed procedure, refer to the "Recovering from LCP ROMMON or an Unstable LCP Image" section of the "Maintaining and Monitoring the Cisco SAMI" chapter of the *Cisco Service Application Module for IP User Guide*.

Miscellaneous Open Caveats

This section lists the miscellaneous caveats that are open in Cisco IOS Release 12.4(15)XQ1.

- CSCso89298

Description: Reconfiguring service-policy under an APN does not work as designed. If the service-policy is removed and reattached, it might stop working.

Workaround: There is currently no known workaround.

- CSCsq14998

Description: During periods of stress condition, when using iSCSI, the Cisco GGSN reloaded. This condition occurred when 120,000 IP PDPs are open and sending bidirectional IMIX at 99k pps, with the CDRs written to iSCSI because the CGW is down. This condition drives the GGSN CPU to 99% usage and after approximately 30 minutes, the GGSN reloaded.

Workaround: There is currently no known workaround.

- CSCsq92712

Description: A SAMI processor might reload when iSCSI-related commands are reconfigured, or unconfigured and configured. This condition can occur when a huge number of pending CDRS (over one million) are being written to the storage device under extremely high signaling and network traffic with CPU and memory utilization of over 90% and 95% respectively.

Workaround: Avoid reconfiguring iSCSI-related commands in extremely high CPU and memory bound conditions.

- CSCsr68717
Description: The SAMI interfaces take a long time to respond to ping packets. Corrupted IPv6 packets are sent to the SAMI.
Workaround: Add IPv6 ACLs in supervisor to stop any IPv6 packets from entering the card. GGSN IPv6 will not be supported once the ACLs are configured.
- CSCta49840
Description: GGSN may run into a fatal error in VPDN/L2TP configurations. This condition may occur in rare race conditions when physical connectivity on interface to LNS is lost while there are active sessions and traffic.
Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(15)XQ1. Only only severity 1 and 2 caveats and select severity 3 caveats are listed.

- [Cisco GGSN Resolved Caveats, page 46](#)
- [Cisco SAMI Resolved Caveats, page 48](#)
- [Miscellaneous Resolved Caveats, page 48](#)

Cisco GGSN Resolved Caveats

This section lists the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(15)XQ1.

- CSCsm20832
Description: On a Cisco router running the Cisco GGSN Release 8.0 software, there is a possibility that the ppp regenerated session count displayed in the output of the **show gprs gtp status** command is incorrect.
- CSCso23232
Description: With the Cisco GGSN, IPv6 PDPs might experience an upstream (from the handset) user data packet loss (not control packet) at a rate of approximately one in 20 million packets.
The packet loss is only observed for packets with the same GTP sequence number between subsequent packets. Ideally, GTP packets carrying user data packets have incrementing sequence numbers in GTP header, and not same GTP sequence number.
- CSCso32048
Description: The Cisco GGSN should log a syslog message when there is a restart count change detected from a remote SGSN, and as a result, PDPs are deleted.
- CSCso37921
Description: The Cisco GGSN Release 8.0 image does not send closed CDRs to iSCSI SAN until the collection timeout, even though the CDR aggregation limit is configured as 1.
- CSCso70877
Description: The Cisco GGSN security Redirect-All feature does not send packets to the configured IP address. This condition occurs for PPP PDPs when the **ip cef** command is enabled. With the **no gprs gtp ip udp ignore checksum** command configured, the Redirect-All feature works as designed.

- CSCso74857

Description: GGSN reloaded at ggsn_client_req_wr_dtr_to_iscsi_san with mixed sig/data under stress conditions where a large number of PDP sessions are created with a high amount of traffic passing through the system, and CDRs are retrieved from an iSCSI target and written to the CGW.
- CSCso84847

Description: If a mobile subscriber includes 3B containing 0x0 at the end of the QoS information element, the Cisco GGSN logs:

```
%GTP-0-GTPv1PACKETPARSINGERROR : GSN: GSN: [IP_address], TEID: [hex], APN: [chars], Reason:The mandatory IE is incorrect and fails the tunnel establishment.
```
- CSCso86579

Description: On a Cisco router running Cisco GGSN Release 8.0 software, the data record format version field of the CDR does not accurately indicate the current version of the 3GPP charging specification supported. The data record format field shows an earlier version although the GGSN supports a later version of the specification. Also, release 7 is not allowed to be configured for the charging release.
- CSCsq24034

Description: The charging version field in the CDR for charging release 4 is 11 instead of 10 when R7 charging is configured.
- CSCsq40129

Description: With an APN for which the Network Behind Ms feature is enabled with AAA authentication performed on RADIUS, a create PDP context request on this particular APN causes the GGSN to reload.
- CSCsq81137

Description: The Cisco GGSN currently does not have a way to send a quota of 0 when the DCCA server is unavailable due to server timeout or when server is down. The GGSN needs to send quota of 0 with cause code of 4 for handling the case of free service.
- CSCsq90817

Description: During the generation of high rate of closed CDRs with iSCSI configured as the charging backup, syslog messages related to GPRS iSCSI are flooding the console with the following message:

```
%GPRISISIFLTMG-4-GPRS_ISCSI_FAILED_ENCODE_AND_STORE: GPRS iSCSI failed to encode and store closed CDRs as the transfer capacity is full
```

This condition is seen when sending high rate of traffic that causes the generation of a high rate of closed CDRs while iSCSI is being used for charging records backup. The traffic rate sent is 80,000 pps (Imix traffic) across the PDPs.
- CSCsr00018

Description: When the Cisco GGSN CPU is driven to 99% usage by bidirectional data packets with charging CDR written to iSCSI (CGW down), the GGSN reloads.
- CSCsr19541

Description: The Cisco GGSN is closing a CDR for an mobile subscriber (MS) time zone change even though there is no change in the MS time zone. This condition occurs when the GGSN receives an update PDP context request.

- CSCsr22641

Symptom: Service aware PDPs cannot be deleted from the GGSN if Service Auth request is received for a service in IDLE state while the PDP is being deleted.

This condition occurs only when the Service Auth request is received for service in IDLE state and the PDP context is being deleted.

- CSCsr41777

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

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

- CSCsr78559

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

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

- CSCsu89644

Description: The Cisco GGSN does not seem to respond to node alive requests sent by the secondary charging gateways using a TCP path. Also, if the node alive request is sent over UDP from the active charging gateway, the GGSN sends the response over TCP if the TCP link is up. This condition occurs with charging gateways using the TCP path.

Cisco SAMI Resolved Caveats

This section lists the Cisco SAMI software caveats that are resolved for Cisco IOS Release 12.4(15)XQ1.

- CSCsk10568

Description: When the Cisco GGSN is under stress (CPU more than 96%), the output of the **show process cpu** command is incorrect.

Miscellaneous Resolved Caveats

This section lists the miscellaneous caveats that are resolved in Cisco IOS Release 12.4(15)XQ1.

- CSCso67108

Description: During periods of stress traffic on the Cisco GGSN, writing to iSCSI causes the GGSN to reload. This condition exists during periods of sustained stress traffic (99% CPU). The iSCSI Tx process not able to allocated buffer and sys logs can be seen—no buffer available -Process= “iSCSI Xmit Process.”

- CSCso55771

Description: CDRs can not be written to an iSCSI disk. This condition occurs after sustained stress traffic that has driven the CPU to 99 percent.

- CSCsr41749

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

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

Caveats - Cisco IOS Release 12.4(15)XQ

This section contains the following types of caveats for Cisco IOS Release 12.4(15)XQ:

- [Open Caveats—Cisco GGSN, page 49](#)
- [Open Caveats—Cisco SAMI, page 50](#)
- [Open Caveats—Other, page 51](#)

Open Caveats—Cisco GGSN

This section documents possible unexpected behavior by Cisco IOS Release 12.4(15)XQ and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsm20832

Description: On a Cisco router running the GGSN Release 8.0 software, there is a possibility of wrong counter for ppp regenerated session count in the output of the **show gprs gtp status** command.

This condition occurs during periods of high traffic load and continuous create and delete PDP context requests. This issue is only with the counter and the virtual-access interfaces as are released for all the PDP contexts.

Workaround: There is currently no known workaround.

- CSCsm95300

Description: With an APN-based steering configuration, if the IP address pool is depleted on one of the reals of the primary serverfarm, the create PDP context requests are not load balanced among the reals of the backup serverfarm.

This condition occurs when a create PDP context request is received and the IP local pool is depleted on a real server (associated to a primary serverfarm), and the CAC notification is sent from the real server to the SLB. This request is, in turn, sent to other reals in the primary serverfarm. If these reals are in “THROTTLED” state, the request is not sent to backup serverfarm.

Workaround: With primary and backup serverfarm configuration, the ip-pool address depletion due to create PDP context requests should not be taking place on the real servers in the primary serverfarm.

- CSCso23232

Description: Its observed that IPv6 PDP might experience an upstream, from the handset, user data packet loss (not control packet) at a rate of approximately one packet in 20 million packets.

The packet loss is only observed for packets with the same GTP sequence number between subsequent packets. Ideally, GTP packets carrying user data packets should have a different/incrementing sequence number in the GTP header and not same the GTP sequence number.

Workaround: There is currently no known workaround.

- CSCso37921

Description: The Cisco GGSN Release 8.0 does not send the closed CDR from the GGSN to iSCSI SAN until the collection timeout, even though the CDR-aggregation limit is configured as 1.

This condition occurs when the iSCSI backup is configured when there are already some closed CDRs in the GGSN memory.

Workaround: Configure low transfer interval timeout, so that when the transfer interval expires, the CDRs are sent to iSCSI SAN.
- CSCso59480

Description: The Cisco GGSN Release 8.0 shows both status and statistics information under the **show gprs iscsi statistics** command. Also, some of the counters are not cleared after clearing them using the **clear gprs iscsi statistics** command.

This condition occurs only when the **show gprs iscsi statistics** command is executed.

Workaround: There is currently no known workaround.
- CSCsy34950

After a reboot, traffic from the user data plane does not leave the Cisco GGSN any longer because no Address Resolution Protocol (ARP) entry exists on the GGSN for the default route (next hop, Cisco CSG2).

This condition occurs only when the **redirect all ip** command is configured when running new CEF code. The new CEF code introduces neighbor resolution optimization (enabled by default) which has issues with ARP packet handling.

Workaround: Disable the optimization by using the **no ip cef optimize neighbor resolution** command on the Cisco GGSN.

Open Caveats—Cisco SAMI

This section lists the Cisco SAMI Software caveats that are open with Cisco IOS Release 12.4(15)XQ.

- CSCsk10568

Description: When the Cisco GGSN is under stress (CPU more than 96%), the output of the **show process cpu** command is incorrect.

Workaround: There is currently no known workaround.
- CSCsk95310

Description: Few packets arrive out of sequence. This condition occurs when a large number of different size packets are sent to the application.

Workaround: There is currently no known workaround.
- CSCsm73343

Description: Packets with an incorrect TCP checksum value are dropped by the gateway. This condition occurs when packets have an incorrect TCP checksum value.

Workaround: There is currently no known workaround.
- CSCsm81174

Description: With more than 500 VRFs configured on a GGSN, a small percentage of packet drop occurs if more than 3 million packets per second are sent to the GGSN, which drives the GGSN CPU utilization as high as 99%.

Workaround: There is currently no known workaround.

Open Caveats—Other

This section lists additional open caveats that are open and apply to Cisco IOS Release 12.4(15)XQ.

- CSCsm36106

Description: Cisco mobile wireless applications using the iSCSI feature will not work when a Logical Unit Numbers (LUN) on an iSCSI target has more than one FAT32 partition. iSCSI works only with a single partition.

This condition occurs when the iSCSI target is configured with more than one partition.

Workaround: Each of the LUNs must have only one FAT32 partition. You can configure more than one LUN on the iSCSI to get multiple FAT32 drives on the initiator.

- CSCsm77433

Description: With APN-based steering, create PDP context requests are not sent via the intended serverfarm.

For example, the first APN is mapped to serverfarm-1, and the second APN is mapped to serverfarm-2. In this scenario, Cisco IOS SLB is sending the create PDP context requests for both of these APNs to serverfarm-1, whereas, the second APN is associated with a serverfarm-2.

This condition occurs if the APN names start with the same string pattern. For example, the first APN name “ip-static” is mapped to serverfarm-1, the second APN name “ip-static-8f” is mapped to serverfarm-2, the create PDP context requests for the second APN are sent to serverfarm-1.

Workaround: When configuring APN steering, ensure that the APN names have unique initial string characters.

- CSCso10535

Description: The Cisco GGSN might reload when changing the policy-map configuration after at least one PDP session is open under an APN which has per-PDP policing applied and traffic over the PDP is being policed.

Workaround: There is currently no known workaround.

- CSCso55171

Description: Spurious memory access while unconfiguring an iSCSI target profile association with the GGSN using the **no gprs iscsi** global configuration command. This condition is observed when the **no gprs iscsi** command is executed while the TCP session with the iSCSI target is down.

Workaround: Unconfigure an iSCSI target profile association from the GGSN while the TCP session is up.

- CSCso55771

Description: CDRs can not be written to an iSCSI disk. This condition occurs after sustained stress traffic that has driven the CPU to 99 percent.

Workaround: There is currently no known workaround.

- CSCso67108

Description: During periods of stress traffic on the Cisco GGSN, writing to an iSCSI device causes the GGSN to reload. This condition exists during periods of sustained stress traffic (99% CPU). The iSCSI Tx process not able to allocated buffer and sys logs can be seen—no buffer available -Process= “iSCSI Xmit Process.”

Workaround: There is currently no known workaround.

Related Documentation

Except for feature modules, documentation is available as printed manuals or electronic documents. Feature modules are available online on Cisco.com.

Use these release notes with these documents:

- [Release-Specific Documents, page 52](#)
- [Platform-Specific Documents, page 52](#)
- [Cisco IOS Software Documentation Set, page 53](#)

Release-Specific Documents

The following documents are specific to Release 12.4 and are located on Cisco.com:

- *Cisco IOS Release 12.4 Mainline Release Notes*
Documentation > Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline > Release Notes
- *Cisco IOS Release 12.4 T Release Notes*
Documentation > Cisco IOS Software > Cisco IOS Software Releases 12.4 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 Cisco.com at <http://www.cisco.com/support/bugtools>.

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:
Documentation > Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline

Platform-Specific Documents

These documents are available for the Cisco 7600 series router platform on Cisco.com and the Documentation CD-ROM:

- *Cisco Service and Application Module for IP User Guide*
- 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*

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 Cisco.com at:

[Documentation](#) > [Cisco IOS Software](#) > [Cisco IOS Software Releases 12.4 Mainline](#) > [Command References](#)

[Documentation](#) > [Cisco IOS Software](#) > [Cisco IOS Software Releases 12.4 Mainline](#) > [Command References](#) > [Configuration Guides](#)



Note

To find a list of MIBs supported by Cisco, by product, see:
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Documentation Roadmap for Implementing GGSN Release 8.0 on the Cisco SAMI

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

General Overview Documents

Core Cisco 7609 Documents:

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

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_roadmap09186a00801ebd9.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 SAMI 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 Service and Application Module for IP User Guide*
http://www.cisco.com/en/US/docs/wireless/service_application_module/sami/user/guide/samiv1.html

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

- Cisco GGSN Release 8.0 Configuration Guide and Command Reference and Associated Release Notes for Cisco IOS Release 12.4(15)XQ.
http://www.cisco.com/en/US/products/sw/wirelssw/ps873/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the *Cisco GGSN Release 8.0 Configuration Guide* and the *Cisco GGSN Release 8.0 Command Reference* publications.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/web/siteassets/legal/trademark.html. Third party trademarks mentioned 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. (1005R)

Copyright © 2011, Cisco Systems, Inc.
All rights reserved.