Release Notes for Cisco GGSN Release 9.*x* on the Cisco SAMI, Cisco IOS Software Release 12.4(22)YE

Publication Date: July 7, 2011

Cisco IOS Release 12.4(22)YE6

This release note describes the requirements, dependencies, and caveats for the Cisco Gateway General Packet Radio Service (GPRS) Support Node (GGSN) Release 9.2, Cisco IOS Release 12.4(22)YE6 on the Cisco Service and Application Module for IP (SAMI). These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4(22)YE, see the "Caveats" section on page 12 and *Caveats for Cisco IOS Release 12.4 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

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

Contents

This release note includes the following information:

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

Cisco GGSN Introduction

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.

General Packet Radio Service (GPRS) and Universal Mobile Telecommunication System (UMTS) are standardized by the European Telecommunications Standards Institute (ETSI). In a GPRS/UMTS packet-switched domain, data services are delivered to the mobile subscriber when a link is established through a Public Land Mobile Network (PLMN) to a GGSN.

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

The Cisco GGSN runs on the Cisco Service and Application Module for IP (SAMI), a new-generation high performance service module for the Cisco 7600 Series Router platforms. For more information about the Cisco SAMI, see the *Cisco Service and Application Module for IP User Guide*.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(22)YE and includes the following sections:

- Memory Recommendations, page 2
- Hardware and Software Requirements, page 3
- Determining the Software Version, page 4
- Upgrading to a New Software Release, page 4

For hardware requirements, such as power supply and environmental requirements and hardware installation instructions, see the *Cisco Service and Application Module for IP User Guide*.

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.4(22)YE

Platforms	Feature Sets	Software Image	Recommended Flash Memory (MB)	Recommended DRAM Memory (GB)	Runs From
Cisco SAMI/ Cisco 7600	GGSN Standard Feature Set	c7svcsami-g8ik9s-mz.124-22.YE6.bin	128	2	RAM

Hardware and Software Requirements

Implementing a Cisco GGSN Release 9.2 on the Cisco 7600 series internet router platform requires the following hardware and software.

- Any module that has ports to connect to the network.
- A Cisco 7600 Series Router and one of the following 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 (WS-SUP720)
  - 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.

  Or one of the following Cisco 7600 series Route Switch Processors running Cisco IOS Release 12.2(33)SRE or later

  - Cisco 7600 Series Route Switch Processor 720 with Distributed Forwarding Card 3C (RSP720-3C-GE)
  - Cisco 7600 Series Route Switch Processor 720 with Distributed Forwarding Card 3CXL (RSP720-3CXL-GE)

  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(22)YE or later.

Note The Cisco GGSN Release 9.*x* software application ships preloaded on the Cisco SAMI processors and is automatically loaded onto each processor during an image upgrade. The Cisco GGSN Release 9.*x* software application supports both the Cisco SAMI 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 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 Second Generation software in each Cisco 7600 Series Router.

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(22)YE6, 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* 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 the *Cisco Service and Application Module for IP User Guide*:

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

MIBs

Platform-Related MIBs

- BGP4-MIB
- CISCO-AAA-SERVER-MIB
- CISCO-BULK-FILE-MIB
- CISCO-CDP-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-FLASH-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-HSRP-EXT-MIB
- CISCO-HSRP-MIB
- CISCO-IMAGE-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-IP-STAT-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
- CISCO-PING-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-QUEUE-MIB
- CISCO-RTTMON-MIB
- CISCO-STACK-MIB
- CISCO-SYSLOG-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
- CISCO-VPDN-MGMT-EXT-MIB
- CISCO-VPDN-MGMT-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- EVENT-MIB
- EXPRESSION-MIB
- IF-MIB
- NOTIFICATION-LOG-MIB
- RMON-MIB

- RSVP-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- TCP-MIB
- UDP-MIB

Application-Related MIBs

- CISCO-GGSN-EXT-MIB
- CISCO-GGSN-GEO-MIB
- CISCO-GGSN-MIB
- CISCO-GGSN-QOS-MIB
- CISCO-GGSN-SERVICE-AWARE-MIB
- CISCO-GPRS-ACC-PT-MIB
- CISCO-GPRS-CHARGING-MIB
- CISCO-GTP-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-ISCSI-MIB

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to:

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 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.

- The number of PDP contexts supported on a GGSN is dependent on the memory and platform in use and the GGSN configuration (for example, whether or not a method of Point-to-Point Protocol [PPP] is configured to forward packets beyond the terminal equipment and mobile termination, if Dynamic Feedback Protocol [DFP] is being used or the memory protection feature is enabled, and the rate of PDP context creation that is 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	384,000
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	16,000	96,000

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

Note Table 2 and Table 3 list the maximum number of PDPs supported when the **no virtual-template subinterface** global configuration command *is not* configured on the GGSN.

With Cisco GGSN Release 8.0 and later, PDPs regenerated to a PPP session run on software interface description blocks (IDBs), which increases the number of sessions the GGSN can support. The GTP virtual template is a subinterface. If the **no virtual-template subinterface** command is configured in global configuration mode, PDPs regenerated to a PPP session run on hardware IDBs instead. When sessions are running on hardware IDBs, the GGSN supports fewer sessions.

- 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 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:

- RADIUS accounting is enabled between the CSG2 and GGSN to populate the Known User Entries Table (KUT) entries with the PDP context user information.
- CSG2 must be configured with the QS addresses of all the GGSN instances.
- Service IDs on the CSG2 are configured as numeric strings that match the category IDs on the Diameter Credit Control Application (DCCA) server.
- If RADIUS is not being used, the Cisco CSG2 is configured as a RADIUS endpoint on the GGSN.
- On the serving GRPS support node (SGSN), the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and CSG2).

  Specifically the SGSN N3*T3 must be greater than:

  2 x RADIUS timeout + *N* x DCCA timeout + 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 can impact slow TCP-based charging paths.

New and Changed Information

The following section lists the new features in the Cisco IOS Release 12.4 YE releases:

- New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE6, page 9
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE5, page 9
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE4, page 9
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE3, page 10
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE2, page 10
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE1, page 11
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE, page 11

For detailed information about the new and existing features in GGSN Release 9.*x*, Cisco IOS Release 12.4 YE releases, refer to the *Cisco GGSN Release 9.x* configuration guide and command reference located at the following URL:

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(22)YE6

There are no new implementations or behavior changes in Cisco IOS Release 12.4(22)YE6.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE5

There are no new implementations or behavior changes in Cisco IOS Release 12.4(22)YE5.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE4

The following new features and behavior change are introduced in Cisco GGSN Release 9.2, Cisco IOS Release 12.4(22)YE4:

- Internet Small Computer System Interface (iSCSI) enhancements
  - The **record-store file-closure-interval** command has been added to provide the option of configuring a file closure interval. To configure an interval, in minutes, at which the GGSN (when writing to an iSCSI target) closes a file and writes data to a new file, use the **record-store file-closure-interval** *mins* command in iSCSI target profile configuration mode.
  - The file-closure-interval field has been added to the **show ip iscsi target** command output. The file-closure-interval field displays the file closure interval configured using the **record-store file-closure-interval** command.
- MIB enhancements

  The following MIBs have been updated with objects related to the Granular Charging, enhanced G-CDRs (eG-CDRs), GTP Session Redundancy (GTP-SR), iSCSI, and Geo-Redundancy features:
  - CISCO-GGSN-MIB
  - CISCO-GGSN-EXT-MIB
  - CISCO-GGSN-GEO-MIB
  - CISCO-GGSN-SERVICE-AWARE-MIB
  - CISCO-GPRS-ACC-PT-MIB
  - CISCO-GPRS-CHARGING-MIB
  - CISCO-GTP-MIB
  - CISCO-HSRP-EXT-MIB

- The following global configuration command has been added to configure the Cisco GGSN behavior when it receives a TPDU 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 the Cisco GGSN receives a GTPv1 TPDU without a sequence number (s=0), it considers the TPDU an out-of-sequence TPDU, and drops it.

  By default this command is not configured, and the default behavior is when the GTPv1 PDP context has reorder_required set to TRUE. If the Cisco GGSN receives a GTPv1 TPDU without a sequence number (s=0), the GGSN allows the TPDU and treats it as a valid TPDU, which does not require reordering and sequence number checks.

  If the PDP context has reorder_required set to FALSE, the GGSN accepts the TPDU without any check for sequence number. In this case, the GGSN accepts both s=0 and s=1). This is an existing behavior and has not changed in Cisco IOS Release 12.4(22)YE4.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE3

There are no new implementations or behavior changes in Cisco IOS Release 12.4(22)YE3.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE2

The following new features and behavior change are introduced in Cisco GGSN Release 9.2, Cisco IOS Release 12.4(22)YE2:

- New Features, page 11
- Behavior Changes, page 11

New Features

Cisco GGSN Release 9.2, Cisco IOS Release 12.4(22)YE2, introduces support of the exchange of service control messages on an *enhanced* quota server interface between the Cisco GGSN and Cisco CSG2.

This support enables the Cisco GGSN to generate eG-CDRs for the following types of users in addition to the service-aware prepaid and service-aware postpaid users supported in releases before Cisco GGSN Release 9.2:

- Service-aware prepaid (GTP') users
- Service-aware postpaid users
- Policy and Charging Control (PCC)-enabled (Gx) users

Note With Cisco IOS Release 12.4(22)YE2 or later, when an enhanced quota server interface is enabled on the GGSN, the GGSN does not function as the quota server for service aware postpaid users or Gx postpaid users, therefore, these uses must be configured as postpaid on the Cisco CSG2. For information about configuring the Cisco CSG2, refer to the *Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide*.

For information about configuring the enhanced quota server interface and enabling support for the exchange of service control messages, refer to the *Cisco GGSN Release 9.2 Configuration Guide.*

Behavior Changes

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(22)YE2 or later to Cisco IOS Release 12.4(22)YE1 or YE, or to Cisco IOS Release 12.4(15)XQ4, XQ3, XQ2, XQ1, or XQ, 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 downgrading the image.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE1

Cisco GGSN Release 9.0, Cisco IOS Release 12.4(22)YE1, introduces support for the following features:

- Layer 3 Geographical Redundancy
- Passive Route Suppression

New Implementations and Behavior Changes in Cisco IOS Release 12.4(22)YE

Cisco GGSN Release 9.0, Cisco IOS Release 12.4(22)YE introduces support for the following features:

- Granular Charging and Storage
- GRX Traffic Segregation
- Gx Interface

- Gy Interface
- Lawful Intercept
- Proxy-CSCF Load Balancing
- Standalone GGSN Prepaid Quota Enforcement

And enhancements to the following existing features:

- Debugging
- DFP Weight
- HSPA QoS Extensions
- MIBs
- Multiple Subnets Behind the Mobile Station
- Statistics

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(22)YE.

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, log in 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(22)YE6

This section contains the following types of caveats that apply to the Cisco GGSN Release 9.2, Cisco IOS Release 12.4(22)YE6 image:

- Open Caveats, page 17
- Resolved Caveats, page 19
- Unreproducible Caveats, page 17

Open Caveats

Note Caveats that are open in a release are also open in 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

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(22)YE6.

- CSCtg44918

  The iSCSI connection closes when the CPU usage is high, and the write function does not work after the connection is restored. The disk goes into an unusable state after the connection is restored.

  This condition occurs when the CPU usage is approximately 70% and the disk size is large (approximately 100 GB). This condition is not seen when the disk size is lower (10 GB or less).

  Workaround: Unconfigure the iSCSI function using the **gprs iscsi** command and then reconfigure the connection.

- CSCtl75759

  The normal burst size in bytes (BC) and excess burst size in bytes (BE) is used for policy PDPs even when BC and BE values are configured under the policy-map.

  This condition occurs on any policy PDP and does not cause a serious result, but rather confusion on why the user configuration does not work. If a user has enough space for a larger token bucket, this condition can effect the user’s ability to optimize system performance.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the SAMI-specific caveats that are open in Cisco IOS Release 12.4(22)YE6.

- CSCsx33840

  The **hw-module module** *module no* **shutdown** command causes the Cisco SAMI to reload rather than shut down. This condition is seen in Cisco SAMI version 03.0(05)SAM and later.

  Workaround: Use the **no power enable module** *mod-num* command on the supervisor to shut down the Cisco SAMI.

Miscellaneous Open Caveats

This section lists the Miscellaneous caveats that are open in Cisco IOS Release 12.4(22)YE6.

- CSCsw62900

  Entries in the cTap2DebugTable are not deleted after the time duration specified in the cTap2DebugAge object. This condition is seen for all debug message entries created in the cTap2DebugTable.

  Workaround: The debug message entries can be manually deleted by setting cTap2DebugStatus object to destroy(6).

Resolved Caveats

- Cisco SAMI Resolved Caveats, page 20
- Cisco SAMI Resolved Caveats, page 20
- Miscellaneous Resolved Caveats, page 21

Cisco GGSN Resolved Caveats

This section list the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(22)YE6.

- 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.

- CSCsy77867

  The transmit counter is not updated in the output of the **show vlans** command for a Gn interface.

- 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.

- CSCtk76072

  The Cisco GGSN running Cisco IOS Software Release 12.4(24)YE1 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.

- 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.

- 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.

- CSCtr61654

  In a redundant implementation, the active GGSN crashes when trying to free the Checkpoint-Facility (CF) buffer when a PDP is being deleted.

- 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.

Cisco SAMI Resolved Caveats

This section list the SAMI-specific caveats that are resolved in Cisco IOS Release 12.4(22)YE6.

- CSCtb83004

  Input queue drops increment every 7-10 seconds on G0/0 with minimal traffic.

  When Layer 2 packets reach the home agents, the **show interface GigabitEthernet 0/0** input queue drops increments with minimal traffic.

  This condition does not impact any data traffic from the mobile nodes.

- 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)
  ```

- CSCtk98031

  After modifying the Internet Small Computer System Interface (iSCSI) configuration, the iSCSI login fails.

  The Cisco SAMI debug shows the following error message:

  ```
  iSCSI ERROR: login error status class 2, status details 7
  ```

  The server log shows the following error message:

  ```
  Initiator did not specify target name in LOGIN request
  ```

Miscellaneous Caveats

This section lists additional miscellaneous caveats that are resolved in Cisco IOS Release 12.4(22)YE6

- CSCtc16985

  Generic Attribute Registration (GARP) packet seen on peer device from unit under test (UUT) interface when the line protocol of the UUT interface is down.

Unreproducible Caveats

This section lists the GGSN-specific caveat that is unreproducible in Cisco IOS Release 12.4(22)YE6.

- CSCti10016

  After the format command is run on a disk larger than 32 GB, the show command displays that only 4 Gbs are free on the device.

  This condition occurs when formatting a disk that is larger than 32 Gb from Cisco IOS software.

- CSCtk66036

  The GGSN connection to the Internet Small Computer System Interface (iSCSI) target fails and the following logs are seen:

```
SAMI 1/3: Oct  9 06:34:11.126 BST: %RSM-4-UNEXPECTED: Error: Drive sda0 unusable (File
inuse in an incompatible mode)
SAMI 1/3: Oct  9 06:34:12.118 BST: %RSM-4-UNEXPECTED: Error: iSCSI target in profile
ISCSI_FWORKSMSA2KT_PROFILE cannot be used for storing/retrieving CDRs. Failed to set
the read/write locations in the disk. Disk is not formatted or is corrupted. Please
format the disk.
SAMI 1/3: Oct  9 06:34:12.118 BST: %GPRSISCSIFLTMG-4-GPRS_ISCSI_OPEN_FAILURE: Unable
to establish session to SAN for target profile ISCSI_FWORKSMSA2KT_PROFILE
```

Caveats - Cisco IOS Release 12.4(22)YE5

This section contains the following types of caveats that apply to the Cisco GGSN Release 9.2, Cisco IOS Release 12.4(22)YE5 image:

- Open Caveats, page 17
- Resolved Caveats, page 19

Open Caveats

Note Caveats that are open in a release are also open in 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

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(22)YE5.

- CSCtg44918

  The iSCSI connection closes when the CPU usage is high, and the write function does not work after the connection is restored. The disk goes into an unusable state after the connection is restored.

  This condition occurs when the CPU usage is approximately 70% and the disk size is large (approximately 100 GB). This condition is not seen when the disk size is lower (10 GB or less).

  Workaround: Unconfigure the iSCSI function using the **gprs iscsi** command and then reconfigure the connection.

- CSCtk76072

  The Cisco GGSN running Cisco IOS Software Release 12.4(24)YE1 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.

  Workaround: There is currently no known workaround.

- CSCtl75759

  The normal burst size in bytes (BC) and excess burst size in bytes (BE) is used for policy PDPs even when BC and BE values are configured under the policy-map.

  This condition occurs on any policy PDP and does not cause a serious result, but rather confusion on why the user configuration does not work. If a user has enough space for a larger token bucket, this condition can effect the user's ability to optimize system performance.

  Workaround: There is currently no known workaround.

- CSCsy77867

  The transmit counter is not updated in the output of the **show vlans** command for a Gn interface.

  Workaround: For the correct data traffic counters, use the **show interface**, **show gprs gtp statistics**, or **show ip traffic** command for the correct data traffic counters.

Cisco SAMI Open Caveats

This section lists the SAMI-specific caveats that are open in Cisco IOS Release 12.4(22)YE5.

- CSCsx33840

  The **hw-module module** *module no* **shutdown** command causes the Cisco SAMI to reload rather than shut down. This condition is seen in Cisco SAMI version 03.0(05)SAM and later.

  Workaround: Use the **no power enable module** *mod-num* command on the supervisor to shut down the Cisco SAMI.

- CSCtb83004

  Input queue drops increment every 7-10 seconds on G0/0 with minimal traffic.

  When Layer 2 packets reach the home agents, the **show interface GigabitEthernet 0/0** input queue drops increments with minimal traffic.

  This condition does not impact any data traffic from the mobile nodes.

  Workaround: There is currently no known workaround.

Miscellaneous Open Caveats

This section lists the Miscellaneous caveats that are open in Cisco IOS Release 12.4(22)YE5.

- CSCsw62900

  Entries in the cTap2DebugTable are not deleted after the time duration specified in the cTap2DebugAge object. This condition is seen for all debug message entries created in the cTap2DebugTable.

  Workaround: The debug message entries can be manually deleted by setting cTap2DebugStatus object to destroy(6).

Resolved Caveats

- Cisco SAMI Resolved Caveats, page 20
- Cisco SAMI Resolved Caveats, page 20
- Miscellaneous Resolved Caveats, page 21
- Unreproducible Caveats, page 21

Cisco GGSN Resolved Caveats

This section list the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(22)YE5.

- 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.

- CSCte68790

  The charging gateway is not able to decode a CDR correctly when the TrafficVolume data contains user location information. This condition occurs because the GGSN does not put the correct length for the userLocationInformation IE.

  This condition occurs with Cisco GGSN Release 9.0 or later, when the PDP context contains user location information. Under these conditions, generated CDRs have the decoding error.

- CSCti07086

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

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

- 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 or later.

- CSCtj72927

  The A-flag is not set in the Cisco GGSN IPv6 router advertisement.

  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.

- CSCtk05719

  Downstream traffic fails at the Cisco GGSN for IPv6 PDP contexts.

  This issue is seen in all Cisco GGSN releases where the IPv6 address is dynamically allocated, and the UE modifies the interface ID.

- CSCtk54730

  GTPv0 PDPs are hanging. This condition occurs when the Cisco GGSN is running Cisco IOS Software Release 12.4(24)YE4 and is specific GTPv0 when an SGSN sends a create request for an already existing PDP associated with a virtual APN.

- CSCtl23238

  When a user starts in a generic radio access network (GRAN) or GSN EDGE Radio Access Network (GERAN), the QoS is either 128 or 472, depending on if the Edge is available or not in GERAN. Then, if the user moves to a location where customer has Universal Terrestrial Radio Access Network (UTRAN) coverage, the SGSN sends the new QoS parameters to the GGSN, but policing is still done on the QoS parameters from the Create PDP Request. All updates appear to be discarded.

Cisco SAMI Resolved Caveats

This section list the SAMI-specific caveats that are resolved in Cisco IOS Release 12.4(22)YE5.

- CSCtg50821

  The crash info file produced by the SAMI application (CSG2, GGSN, etc.) is either be empty or contains files with limited or no content.

  This condition occurs only when the application is crashing due to some other unrelated defect.

- CSCtj12698

  In a redundant Cisco SAMI configuration, the “RF induced reload” error message and a traceback display on the supervisor engine when the Cisco SAMI is reloaded or reset.

- CSCtj92505

  A Cisco SAMI processor reloads saying Rf-INTERDEV self-induced reload. This condition occurs when the implementation is redundant and there is a momentary communication breakdown between the SAMI processors.

Miscellaneous Resolved Caveats

This section lists additional miscellaneous caveats that are resolved in Cisco IOS Release 12.4(22)YE5

- CSCsy55362

  The console could stop responding when the TACACS+ server is used as an AAA server and the single connection option is configured.

- CSCsy84312

  In a redundant implementation, the Cisco SAMI application is not able to write to the core file when forced to crash with the process watchdog timeout option.

- CSCta49840

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

- CSCtd93883

  In a redundant implementation, a few processes in RF running even after a crash leads to a reload of the box.

- 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.

Unreproducible Caveats

This section lists the GGSN-specific caveat that is unreproducible in Cisco IOS Release 12.4(22)YE5.

- CSCth29522

  The signaling SGSN address is not synchronized to the standby GGSN when the SGSN sends different recovery IEs in quick succession.

  This issue is seen when the following conditions occur:

  1. The SGSN restarts multiple times and sends a create PDP context request for the same IMSI with different signaling SGSN IP addresses and also a different restart counter in the recovery IE.
  2. Echo timing is not configured on the Gn path. When Gn path has echo timing configured, this issue is seen only if the SGSN recovers or reloads within the echo interval (default 60 seconds).

Caveats - Cisco IOS Release 12.4(22)YE4

This section contains the following types of caveats that apply to the Cisco GGSN Release 9.2, Cisco IOS Release 12.4(22)YE4 image:

- Open Caveats, page 22
- Resolved Caveats, page 24

Open Caveats

Note Caveats that are open in a release also are open in 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 22
- Cisco SAMI Open Caveats, page 23
- Miscellaneous Open Caveats, page 23

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(22)YE4.

- CSCsy77867

  The transmit counter is not updated in the output of the **show vlans** command for a Gn interface.

  Workaround: For the correct data traffic counters, use the **show interface**, **show gprs gtp statistics**, or **show ip traffic** command for the correct data traffic counters.

- CSCtg44918

  The iSCSI connection closes when the CPU usage is high, and the write function does not work after the connection is restored. The disk goes into an unusable state after the connection is restored.

  This condition occurs when the CPU usage is approximately 70% and the disk size is large (approximately 100 GB). This condition is not seen when the disk size is lower (10 GB or less).

  Workaround: Unconfigure the iSCSI function using the **gprs iscsi** command and then reconfigure the connection.

- CSCtg59859

  The cHsrpExtIfTrackedIpNone object is not fetching when trying to get cHsrpExtIfStandbyTable objects. This condition is seen when the **standby** [*group-number*] **track** *interface-type interface-numbe*r [*interface-priority*] command is not configured.

  Workaround: Ensure that the **standby** [*group-number*] **track** *interface-type interface-numbe*r [*interface-priority*] command and the **standby [***group-number***] ip none** command are configured before querying the cHsrpExtIfTrackedIpNone object.

- CSCth10867

  A GPRS iSCSI error message displays when a charging group is unconfigured. This condition occurs when an iSCSI target is configured under the charging group.

  Workaround: Unconfigure the iSCSI target associated with a charging group before unconfiguring the charging group. First unconfigure iscsi and then charging group,

- CSCth13357

  Large number of failed read requests occurring during iSCSI read operation. This condition occurs when the Cisco GGSN is sending an extra read request even though it has received an empty record in a previous read request.

  Workaround: There is currently no known workaround.

- CSCth29522

  The signaling SGSN address is not synchronized to the standby GGSN when the SGSN sends different recovery IEs in quick succession.

  This issue is seen when the following conditions occur:

  3. The SGSN restarts multiple times and sends a create PDP context request for the same IMSI with different signaling SGSN IP addresses and also a different restart counter in the recovery IE.
  4. Echo timing is not configured on the Gn path. When Gn path has echo timing configured, this issue is seen only if the SGSN recovers or reloads within the echo interval (default 60 seconds).

  Workaround: Ensure that the Gn path echo is set to the default (60 seconds). If the Gn path echo is set to the default, the chances of this issue occurring is very remote because the PDP context will be deleted on the GGSN before the SGSN recovers. Therefore, the create request sent after the SGSN recovers will be a fresh create request. If the mismatch has already occurred, reload the standby node to ensure that the correct value is synchronized to the standby during the bulk synchronization.

Cisco SAMI Open Caveats

This section lists the SAMI-specific caveats that are open in Cisco IOS Release 12.4(22)YE4.

- CSCsx33840

  The **hw-module module** *module no* **shutdown** command causes the Cisco SAMI to reload rather than shut down. This condition is seen in Cisco SAMI version 03.0(05)SAM and later.

  Workaround: Use the **no power enable module** *mod-num* command on the supervisor to shut down the Cisco SAMI.

- CSCtb83004

  Input queue drops increment every 7-10 seconds on G0/0 with minimal traffic.

  When Layer 2 packets reach the home agents, the **show interface GigabitEthernet 0/0** input queue drops increments with minimal traffic.

  This condition does not impact any data traffic from the mobile nodes.

  Workaround: There is currently no known workaround.

Miscellaneous Open Caveats

This section lists the Miscellaneous caveats that are open in Cisco IOS Release 12.4(22)YE4.

- CSCsw62900

  Entries in the cTap2DebugTable are not deleted after the time duration specified in the cTap2DebugAge object. This condition is seen for all debug message entries created in the cTap2DebugTable.

  Workaround: The debug message entries can be manually deleted by setting cTap2DebugStatus object to destroy(6).

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(22)YE4. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco GGSN Resolved Caveats, page 24
- Cisco SAMI Resolved Caveats, page 26
- Miscellaneous Resolved Caveats, page 26

Cisco GGSN Resolved Caveats

This section list the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(22)YE4.

- CSCta53732

  Under very rare conditions, the Cisco GGSN might end up with stale PDP contexts when different GTP version create PDP context requests with different Restart values are received from different SGSNs (signaling and data different), and the different restart values are received within a duration of less than 60 seconds.

- CSCtd43472

  When an iSCSI connection is up, the format of the bootflash generates a traceback.

- 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 sychronized 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.

- 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.

- 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.

- CSCte95900

  The iSCSI session fails to come up when iSCSI is configured under a charging group and the Cisco GGSN has received a fatal error. This condition is only seen when a target profile name is 7 characters (for example, TRIAL-1), which leads to memory corruption.

- CSCtf16844

  A fatal error might occur while when unconfiguring an iSCSI target using the **no ip iscsi target** command. This condition occurs when an iSCSI session is in a failed state and the user attempts to unconfigure the target.

- CSCtf20248

  The Cisco GGSN permits adding, removing, or modifying the **gprs charging source interface** command when the charging gateways are configured.

- CSCtf68451

  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(22)YE4" section on page 9.

- 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.

- CSCtf80645

  When service-aware billing is enabled on the GGSN using the **gprs service-aware** command, Lawful Intercept does not work.

  This condition occurs with only GTPv1 when the following configuration exists:

  a. The GGSN has a service-aware transparent APN configuration.

  b. Standalone GGSN Prepaid quota enforcement is enabled on the GGSN using the **gprs prepaid stand-alone** command.

- CSCtg55670

  When the enhanced quota server interface between the GGSN and Cisco CSG2 is configured to enable the exchange of service control messages that enable the GGSN to generate enhanced G-CDRs (eG-CDRs) for service-aware prepaid GTP' users, a memory leak occurs on the standby GGSN. The memory leak eventually causes the standby GGSN to reload.

  Related configuration commands on GGSN include the **ggsn quota-server** *server-name* **service-msg** command and the **charging record type egcdr** command.

  The active GGSN is not impacted by this issue, except for some temporary additional processing required to synchronize state information from the active to the standby GGSN once the standby GGSN has completed reloading. In addition, the service-aware Gy/CLCI prepaid functionality and configuration on the GGSN is not impacted by this issue.

- CSCtg65496

  A service-aware prepaid session fails due to an invalid Credit Control Record (CCR).

  This condition occurs when the DCCA interface is not configured with the **gprs dcca clci** command or the **gprs dcca 3gpp** command, and the OCS server is based on a DCCA interface compatible with non VF-CLCI (the default in Cisco GGSN Release 8.0 and prior versions).

- CSCtg67391

  In some scenarios, sending a SCSI command header and NOP OUT over a TCP connection fails because these scenarios are not properly handled. This condition can lead to fatal error.

  This condition occurs when the TCP task is consumed with other TCP traffic in parallel to the iSCSI writes. The condition surfaces when the TCP connection does not have enough buffer to cater to the requests over TCP.

Cisco SAMI Resolved Caveats

There are no newly resolved SAMI caveats with Cisco IOS Release 12.4(22)YE4.

Miscellaneous Resolved Caveats

This section lists additional miscellaneous caveats that are resolved in Cisco IOS Release 12.4(22)YE4

- CSCtd86472

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCte14603

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

- CSCte69879

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

- CSCtf05217

  When a single Open Shortest Path First (OSPF) process is removed, the Cisco GGSN **passive-interface** *interface* **on-standby** command is removed from all OSPF processes.

- CSCtf06284

  After the Cisco GGSN transitions from standby to active, the SNMP counters for the cgprsAccPtStatisticsEntry and cGgsnStatistics objects are incorrect. This condition is seen only after a transition from standby GGSN to active GGSN.

- CSCtf17624

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- 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).

- CSCtg27136

  The scada gateway feature enable or disable commands do not work (**scada gateway** command and **no scada gateway** command).

Caveats - Cisco IOS Release 12.4(22)YE3

This section contains the following types of caveats that apply to the Cisco GGSN Release 9.2, Cisco IOS Release 12.4(22)YE3 image:

- Open Caveats, page 37
- Resolved Caveats, page 40

Open Caveats

Note Caveats that are open in a release also are open in 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 32
- Cisco SAMI Open Caveats, page 33
- Miscellaneous Open Caveats, page 33

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(22)YE3:

- CSCsy77867

  The transmit counter is not updated in the output of the **show vlans** command for a Gn interface.

  Workaround: For the correct data traffic counters, use the **show interface**, **show gprs gtp statistics**, or **show ip traffic** command for the correct data traffic counters.

- CSCsy81406

  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 known caveats open in Cisco IOS Release 12.4(22)YE3.

Miscellaneous Open Caveats

This section lists the Miscellaneous caveats that are open in Cisco IOS Release 12.4(22)YE3.

- CSCsw62900

  Entries in the cTap2DebugTable are not deleted after the time duration specified in the cTap2DebugAge object. This condition is seen for all debug message entries created in the cTap2DebugTable.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(22)YE3. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco GGSN Resolved Caveats, page 33
- Cisco GGSN Closed or Unreproducible Caveats, page 30
- Cisco SAMI Resolved Caveats, page 30
- Miscellaneous Resolved Caveats, page 31

Cisco GGSN Resolved Caveats

This section list the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(22)YE3.

- CSCtc59307

  The Internet Small Computer System Interface (iSCSI) session fails to come up with an "Unknown iscsi pdu type" error message. The file system is deleted, and the iSCSI target device is not usable for reading or writing charging detail records (CDRs).

  This condition is seen only when data greater than the MaxBurstSize negotiated during the iSCSI login phase is written to the target.

- CSCtd26872

  After the Cisco GGSN is reloaded, the charging gateway might not come up as active. This condition might occur when the Cisco GGSN reloads because of a user-initiated reset or because a fatal error occurs, and the charging gateway does not send a node alive.

- CSCtd58773

  PDP contexts are always being configured with the default BC and BE values, even when BC and BE configurations are entered by the user under the policy-map. This condition is seen on any policy PDP.

- CSCtd59007

  Cisco GGSN Release 9.0 displays an increased CPU utilization over Cisco GGSN Release 8.0 when simultaneous create PDP context requests and update PDP context requests are processed by the GGSN, and the GGSN is configured for service-aware CLCI prepaid with Gn-side triggers active.

- CSCtd59216

  The **clear gprs gtp debug next-call** *tid* command might delete the wrong PDP context from the list of nextcall debugged PDPs.

  This condition occurs if the PDP TID has zeros preceding other digits (for example, 1023 and 1024). The first PDP in the list is deleted.

- CSCtd68918

  If the number of PDPs is less than 100, counters are updated immediately and the values in the **show** output show the most recent global counters. If the number of PDPs is greater than 100, and the **show** command is issued multiple times within 15 seconds, the output shows data that is 15 seconds old.

- CSCte17430

  The **no debug condition called** command does not reset the APN flag. This condition occurs when conditional debugging is set using the **debug condition called apn.com**.

- CSCte45575

  The active GGSN SAMI PPC resets at the same time the standby GGSN SAMI PPC resets.

  This condition occurs when:

  - Each Cisco SAMI PPC has its own IP address (non Single IP applications)
  - The reload is initiated either from the supervisor engine module or the Cisco SAMI Line Control Processor (LCP) (not when reloaded from the Cisco SAMI PPC)
  - The standby GGSN has a higher HSRP priority, or has a higher physical interface IP address than the active GGSN.

- CSCte53024

  The Cisco GGSN sends CDRs to the charging gateway that contain invalid headers.

  When the **gprs auto-retrieve** command is configured on the Cisco GGSN, and the path to the charging gateway is flip-flopping and iSCSI traffic is slowing down at the same time, the CDR recovered from iSCSI might not contain a valid header.

- CSCte71467

  When connected to a Linux target, the iSCSI session fails to come up and a fatal error occurs on the Cisco GGSN. This condition is seen only when the iSCSI target profile name is seven characters long (for example, TRIAL-1), which leads to memory corruption.

- 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.

Cisco GGSN Closed or Unreproducible Caveats

This section list the GGSN-specific caveats that are closed or unreproducible in Cisco IOS Release 12.4(22)YE3.

- CSCta58607

  Although the redundancy states Active-Standby are established, the **reload peer** command does not reload the peer. Debugs show that peer is reloaded upon redundancy **reload peer** command execution.

- CSCtd74493

  The Cisco GGSN does not create a new PDP for an existing one when there is a conflict of IP address for mobile station. Instead, the GGSN waits for the retransmission for the create PDP context request to be successful.

  Workaround: There is currently no known workaround, however, in production deployment, there are typically retransmissions for a create PDP context request.

Cisco SAMI Resolved Caveats

There are no newly resolved SAMI caveats with Cisco IOS Release 12.4(22)YE3.

Miscellaneous Resolved Caveats

This section lists additional miscellaneous caveats that are resolved in Cisco IOS Release 12.4(22)YE3.

- 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 HSRP.

- CSCsz19104

  When an active device is reloaded using the **reload** command, HSRP might go through an unnecessary transition that causes a standby reload as well.

  This condition can occur when:

  - Using redundancy inter-device, or with an unexpected HSRP transition
  - Issuing the **reload** command from the active SAMI PPC
  - The active master HSRP has a higher HSRP priority, or higher physical interface IP address
  - Using smaller non-default HSRP timer values (for example, this condition is seen with standby timers 1 3)

- CSCtb13421

  The GM might not register. This condition has been seen after an interface is shutdown when a crypto map with a local address is configured and applied to multiple interfaces.

- CSCte53683

  iSCSI sporadic write failures occurs with the EMC Celerra NX4. This condition is seen after upgrading to the Cisco GGSN Release 9.0, Cisco IOS 12.4(22)YE1 image.

- CSCtf07557

  File creation or file delete sporadically fails with a “File In Use in Incompatible mode” error message. This condition occurs when file create and delete operations are executed simultaneously on the same path and both files have the same first six characters.

Caveats - Cisco IOS Release 12.4(22)YE2

This section contains the following types of caveats that apply to the Cisco GGSN Release 9.2, Cisco IOS Release 12.4(22)YE2 image:

- Open Caveats, page 37
- Resolved Caveats, page 40

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 32
- Cisco SAMI Open Caveats, page 33
- Miscellaneous Open Caveats, page 33

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(22)YE2:

- CSCsy77867

  The transmit counter is not updated in the output of the **show vlans** command for a Gn interface.

  Workaround: For the correct data traffic counters, use the **show interface**, **show gprs gtp statistics**, or **show ip traffic** command for the correct data traffic counters.

- CSCsy81406

  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.

- CSCta58607

  Although the redundancy states Active-Standby are established, the **reload peer** command does not reload the peer. Debugs show that peer is reloaded upon redundancy **reload peer** command execution.

  Workaround: Execute the reload on the peer by logging into the console.

- CSCtd26872

  The charging gateway might not come up as active following a reload of the GGSN.

  Workaround: Unconfigure and reconfigure the charging gateway or issue a node alive message from the charging gateway.

- CSCtd72030

  The creation of PDP contexts fails for PPP-layer 2tunneling protocol (L2TP) type PDPs. The create PDP response might reach the SGSN, but some GGSN **show** command do not display the PDP context. In addition, sending traffic to such a PDP might result in the GGSN reloading.

  Workaround: There is currently no known workaround.

- CSCtd74493

  The Cisco GGSN does not create a new PDP for an existing one when there is a conflict of IP address for mobile station. Instead, the GGSN waits for the retransmission for the create PDP context request to be successful.

  Workaround: There is currently no known workaround, however, in production deployment, there are typically retransmissions for a create PDP context request.

Cisco SAMI Open Caveats

There are no known caveats open in Cisco IOS Release 12.4(22)YE2.

Miscellaneous Open Caveats

This section lists the Miscellaneous caveats that are open in Cisco IOS Release 12.4(22)YE2.

- CSCsw62900

  Entries in the cTap2DebugTable are not deleted after the time duration specified in the cTap2DebugAge object. This condition is seen for all debug message entries created in the cTap2DebugTable.

  Workaround: Manually delete the debug message entries by setting the cTap2DebugStatus object to 6 (destroy).

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(22)YE2. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco GGSN Resolved Caveats, page 33
- Cisco SAMI Resolved Caveats, page 35
- Miscellaneous Resolved Caveats, page 35

Cisco GGSN Resolved Caveats

This section list the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(22)YE2.

- CSCsz96787

  Description: When a loopback interfaces is configured as the charging source address, and GGSN service has been disabled using the **no gprs service** global configuration command, the loopback interface cannot be unconfigured.

- 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.

- CSCta34630

  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

  Under very rare conditions, the Cisco GGSN might end up with stale PDP contexts when different GTP version create PDP context requests with different Restart values are received from different SGSNs (signaling and data different), and the different restart values are received within a duration of less than 60 seconds.

- CSCta95578

  A Cisco router running the Cisco GGSN software made a spurious memory access while trying to send an Simple Network Management Protocol (SNMP) trap when PDP contexts were rejected due to low memory. This condition occurs only when the PDP contexts are rejected due to low memory and traps were configured.

- CSCtb03235

  The APN counter is not incremented as expected under the **show gprs charging status charging-group <>** command output. This condition is seen with the following steps:

  Configure Charging-group (CGG1) under APN1 and disable charging globally.

  2) Create PDP context for APN1 and make sure it is not generating any CDRs.

  3) Delete the PDP context.

  4) Enable charging in GGSN and create a PDP context. Make sure the PDP is generating CDRs.

- CSCtb77302

  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

  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 over with GTPv1.

- CSCtc07857

  Under rare conditions, a fatal error might occur with GTP parsing of PPP.

- CSCtc34938

  Some Cisco GGSN processors on the standby SAMI reload with an “RF induced self-reload” syslog message.

Cisco SAMI Resolved Caveats

This section lists the Cisco SAMI software caveats that are resolved in Cisco IOS Release 12.4(22)YE2.

- CSCsw74149

  I/O memory depleted if a packet has ICMP source and destination IP addresses that are the same as the PPC interface IP address

  If a packet has an ICMP source and destination IP address that is the same as the PPC interface IP address, the SAMI runs out of I/O memory, and the following message appears:

  %SYS-2-MALLOCFAIL: Memory allocation of 1708 bytes failed from 0x45407D18, alignment 32

- CSCsz86656

  The Cisco SAMI does not set the DBUS trust bit to 1, which in turn causes the Cisco 7600 series router to remark the DSCP of the packets.

Miscellaneous Resolved Caveats

This section lists additional caveats that are resolved in Cisco IOS Release 12.4(22)YE2.

- 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.

- 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 webpage.

  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

- CSCsz45567

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

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

- CSCsz48614

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCsz48680

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled. Remote code execution may also be possible.

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

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

- CSCsz49741

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCsz75186

  Cisco IOS Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang. The vulnerability may be triggered by a TCP segment containing crafted TCP options that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability.

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

- CSCsz89904

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled. Remote code execution may also be possible.

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

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

- CSCta19962

  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.

- 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.

Caveats - Cisco IOS Release 12.4(22)YE1

This section contains the following types of caveats that apply to Cisco GGSN Release 9.2, Cisco IOS Release 12.4(22)YE1 image:

- Open Caveats, page 37
- Resolved Caveats, page 40

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 38
- Cisco SAMI Open Caveats, page 40
- Miscellaneous Open Caveats, page 40

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(22)YE1.

- CSCsy77867

  The transmit counter is not updated in the output of the **show vlans** command for a Gn interface.

  Workaround: For the correct data traffic counters, use the **show interface**, **show gprs gtp statistics**, or **show ip traffic** command for the correct data traffic counters.

- CSCsy91211

  The Cisco GGSN is unable to establish a session with the iSCSI target due to low memory. This condition occurs when there is a continuous, and higher rate of generated closed CDRs on the GGSN than the GGSN-to-iSCSI transfer rate can handle, leading to CDR accumulation on the GGSN.

  Workaround: To ensure that the Cisco GGSN has sufficient memory to establish an iSCSI session to drain the pending CDRs, set the GGSN CDR triggers properly to avoid long durations of generated closed CDRs. Additionally, configure the GGSN memory trap so that when the GGSN reaches its memory threshold, no additional PDP sessions are sent into the GGSN using SLB DFP.

- CSCsy44803

  In a redundant configuration, a new Standby Cisco SAMI (formerly the Active SAMI) might perform an extra reload.

  This condition occurs with an Active-Standby configuration after a switchover. The extra reload is seen intermittently, with approximately 3 percent of switchovers.

  Workaround: There is currently no known workaround.

- CSCsy81406

  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.

- CSCsz81712

  When the Cisco GGSN charging service mode is moved from operational to maintenance, and then back to operational while call data records (CDRs) are being written to the iSCSI backup target, a few CDRs might get written to the iSCSI target twice.

  Workaround: There is currently no known workaround.

- 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.

  Workaround: Manually clear the PDP context using the **clear gprs gtp pdp-context** command.

- CSCta34630

  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.

  Workaround: There is currently no known workaround.

- CSCta53732

  Under very rare conditions, the Cisco GGSN might end up with stale PDP contexts when different GTP version create PDP context requests with different Restart values are received from different SGSNs (signaling and data different), and the different restart values are received within a duration of less than 60 seconds.

  Workaround: There currently is no known workaround.

- CSCta58607

  Although the redundancy states Active-Standby are established, the **reload peer** command does not reload the peer. Debugs show that peer is reloaded upon redundancy **reload peer** command execution.

  Workaround: Execute the reload on the peer by logging into the console.

- CSCta66024

  The Cisco GGSN does not remove the path to the secondary charging gateway even after the gateway is down.

  Workaround: There is no known workaround.

- CSCta77830 The Cisco GGSN does not respond to a PDP status query when the corresponding PDP context is deleted in the GGSN.

  Workaround: Wait until the configured number of status queries before deleting the corresponding PDP.

- CSCta78195

  The new Standby Cisco SAMI (formerly Active Cisco SAMI) might perform an extra reload after a switchover. This reload is seen intermittently after an Active-Standby switchover (approximately 3%).

  Workaround: There is currently no known workaround.

- CSCta86513

  The “umts qos_neg” field displayed when the **show gprs gtp pdp tid <>** executed is not expected after sending a COA update.

  Workaround: There is currently no known workaround.

- CSCta95578

  Cisco router running the Cisco GGSN software made a spurious memory access while trying to send an SNMP trap when PDP contexts were rejected due to low memory. This condition occurs only when the PDP contexts are rejected due to low memory and traps were configured.

  Workaround: There is currently no known workaround.

- CSCtb03235

  The APN counter is not incremented as expected under the **show gprs charging status charging-group <>** command output. This condition is seen with the following steps:

  Configure Charging-group (CGG1) under APN1 and disable charging globally.

  2) Create PDP context for APN1 and make sure it is not generating any CDRs.

  3) Delete the PDP context.

  4) Enable charging in GGSN and create a PDP context. Make sure the PDP is generating CDRs.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the SAMI-specific caveats that are open in Cisco IOS Release 12.4(22)YE1.

- CSCsz86656

  The Cisco SAMI does not set the DBUS trust bit to 1, which in turn causes the Cisco 7600 series router to remark the DSCP of the packets.

Miscellaneous Open Caveats

This section lists the Miscellaneous caveats that are open in Cisco IOS Release 12.4(22)YE1.

- CSCsw62900

  Entries in the cTap2DebugTable are not deleted after the time duration specified in the cTap2DebugAge object. This condition is seen for all debug message entries created in the cTap2DebugTable.

  Workaround: Manually delete the debug message entries by setting the cTap2DebugStatus object to 6 (destroy).

Resolved Caveats

The following sections list caveats that have been resolved with Cisco IOS Release 12.4(22)YE1. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco GGSN Resolved Caveats, page 40
- Cisco SAMI Resolved Caveats, page 44
- Miscellaneous Resolved Caveats, page 45

Cisco GGSN Resolved Caveats

This section list the GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(22)YE1.

- 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.

- CSCsr18691

  Cisco IOS devices that are configured with Cisco IOS Zone-Based Policy Firewall Session Initiation Protocol (SIP) inspection are vulnerable to denial of service (DoS) attacks when processing a specific SIP transit packet. Exploitation of the vulnerability could result in a reload of the affected device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available within the workarounds section of the posted advisory.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-ios-fw.shtml

- 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.

- CSCsu24505

  Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available and are documented in the workarounds section of the posted advisory.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml

- CSCsu50252

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsu70214

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsv48603

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsv75948

  Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available and are documented in the workarounds section of the posted advisory.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml

- 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.

- CSCsw87426

  cTap2StreamInterceptEnable cannot be set to True (enabled) unless a stream is added and set to active. However, when the stream is deleted, cTap2StreamInterceptEnable remains in a True state when it should be set to False (disabled), or alternatively, the True state should prevent the stream from being deleted.

- CSCsx07114

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- 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.

- CSCsx25880

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml.

- CSCsx70889

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tunnels.shtml.

- 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.

- CSCsy48122

  Spurious memory access error message and tracebacks related to UMTS service policy might occur during PDP context creation. This condition might occur when PDPs with police and CAC policy are created and deleted, and the police policy is then unconfigured. The traceback might be seen when the PDP context is recreated.

- CSCsy50495 - GGSN Reloads while configuring service gprs ggsn after running some test

  The Cisco GGSN sometimes reloads when starting and stopping s**ervice gprs ggsn**. This condition was seen after running a prepaid standalone feature test script, unconfiguring service gprs ggsn, and running a similar prepaid script again by first enabling **service gprs ggsn**.

- CSCsy54122

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsy92690

  For a service-aware PDP, the CDR is closed for every service record due to an “sgsn-change,” with a closure cause as **sgsn-change** when an update request is received with an SGSN change.

  This condition occurs when the categories are armed with the SGSN trigger, and also only when the sgsn-change-limit is disabled or configured to a value anything other than 0 in the charging profile.

- CSCsy93161

  An extra Framed-Route is added as a Network-Behind-MS (NBMS) route in certain scenarios. This Framed-Route appears as first the NBMS route.

  This condition occurs after the following sequence of events:

  - The Network-Behind-Mobile is configured under the APN.
  - RADIUS returns a Framed-Mask less than 32 bits.
  - The extra route comprises a network range of Framed-IP-Address + Framed-Mask.

- CSCsz01114

  On charging gateway switchover, the Cisco GGSN sends pending and closed CDRs to the new active charging gateway only after charging collection timer expires.

- CSCsz14014

  The Cisco GGSN increments successful dynamic IPv6 PDP activation counter displayed under **show gprs access-point statistics** command, even when the IPv6 create PDP context request contains an invalid user. This issue is seen only for IPv6 PDPs.

- CSCsz24898

  The Cisco GGSN does not CEF switch down-link data traffic when the PPP-Regeneration **allow-duplicate** option is used. This condition is seen for any PDPs created when the PPP-Regeneration **allow-duplicate** option is used, even when the PDP addresses are unique.

- CSCsz32043

  If a new incoming PDP hits more than one set next-call debug condition, it will remove all of them rather than only remove one according to the priority. If a new incoming PDP hits more than one set next-call debug conditions, it will remove all of them rather than only remove one according to the priority.
- CSCsz33490

  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.
- CSCsz57600 - Change CISCO-GGSN-EXT-MIB OID to ciscoMgmt 647

  The CISCO-GGSN-EXT-MIB is not accessible on Cisco GGSN Release 9.0 when the MIB is queried using the OID, 1.3.6.1.4.1.9.9.647.
- CSCsz66875

  A traceback seen in the Cisco GGSN after reloading the Cisco SAMI.
- CSCta02056

  A PPP session setup failed because of a missing sequence number in the T-PDU packet.
- CSCta16716

  A traceback is shown while reloading the Cisco GGSN. This reload only occurs with a route reload with a Cisco GGSN image that does not have service gprs ggsn configured.
- CSCta42124

  The Cisco GGSN rejects any charging message when the charging source is configured under VRF. This condition occurs only when the charging source interface is configured under VRF.
- CSCta72589

  There is traceback seen when configuring **service gprs ggsn**. This condition occurs when the ggsn service is removed (no **service gprs ggsn**) and then reconfigured (**service gprs ggsn**).
- CSCtb09757

  The Cisco GGSN running the Release 9.0 image encounters a CPU spike on the SNMP-ENGINE process when a snmpwalk is made over ciscoGprsAccPtMIB. This condition occurs when querying ciscoGprsAccPtMIB when there are existing PDPs.

Cisco SAMI Resolved Caveats

This section lists the Cisco SAMI software caveats that are resolved in Cisco IOS Release 12.4(22)YE1.

- CSCsy65876

  Some debug information, such as **show tech** and **show sami config-mode**, might be missing from the debug-info files that generate prior to a reload following a critical error. This failure to collect all debug-info files rarely occurs, and the condition under which it occurs is unknown.

Miscellaneous Resolved Caveats

This section lists additional caveats that are resolved in Cisco IOS Release 12.4(22)YE1.

- CSCsz06768

  On Cisco GGSN R9.0, when the **show record-storage-module target-info all detail** command is executed while an iSCSI session is being torn down, spurious memory access is observed. The spurious memory access is observed only when the **show** command output is displayed while the iSCSI session is being torn down and terminal length is not 0.

- 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.

Caveats - Cisco IOS Release 12.4(22)YE

This section contains the following types of caveats that pertain to Cisco IOS Release 12.4(22)YE.

Open Caveats—Cisco GGSN

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

This section documents possible unexpected behavior by Cisco IOS Release 12.4(22)YE and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsw62900

  Entries in the cTap2DebugTable are not deleted after the time duration specified in the cTap2DebugAge object. This condition is seen for all debug message entries created in the cTap2DebugTable.

  Workaround: Manually delete the debug message entries by setting the cTap2DebugStatus object to 6 (destroy).

- 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.

  Workaround: Manually clear the PDP contexts using the **clear gprs gtp pdp-context** command.

- CSCsy33164

  A reload of a Standby GGSN causes the Active GGSN to reload. This condition occurs with HSRP version 2 when different HSRP standby group numbers are configured on the interfaces.

  Workaround: Follow the recommended configuration for HSRP for GTP Session Redundancy, which is to use the same standby group number for all interfaces.

- CSCsy44803

  In a redundant configuration, a new Standby Cisco SAMI (formerly the Active SAMI) might perform an extra reload.

  This condition occurs with an Active-Standby configuration after a switchover. The extra reload is seen intermittently, with approximately 3 percent of switchovers.

  Workaround: There is no known workaround.

- CSCsy48122

  Spurious memory access error message and tracebacks related to UMTS service policy might occur during PDP context creation. This condition might occur when PDPs with police and CAC policy are created and deleted, and the police policy is then unconfigured. The traceback might be seen when the PDP context is recreated.

  Workaround: To avoid the spurious memory access message and tracebacks, do not remove UMTS service policies once they are configured under the APN.

- CSCsy77867

  The transmit counter is not updated in the output of the **show vlans** command for a Gn interface.

  Workaround: For the correct data traffic counters, use the **show interface**, **show gprs gtp statistics**, or **show ip traffic** command for the correct data traffic counters.

- CSCsy81406

  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.

- CSCsy91211

  The Cisco GGSN is unable to establish a session with the iSCSI target due to low memory. This condition occurs when there is a continuous, and higher rate of generated closed CDRs on the GGSN than the GGSN-to-iSCSI transfer rate can handle, leading to CDR accumulation on the GGSN.

  Workaround: To ensure that the Cisco GGSN has sufficient memory to establish an iSCSI session to drain the pending CDRs, set the GGSN CDR triggers properly to avoid long durations of generated closed CDRs. Additionally, configure the GGSN memory trap so that when the GGSN reaches its memory threshold, no additional PDP sessions are sent into the GGSN using SLB DFP.

- CSCsy93161

  An extra Framed-Route is added as a Network-Behind-MS (NBMS) route in certain scenarios. This Framed-Route appears as first the NBMS route.

  This condition occurs after the following sequence of events:

  - The Network-Behind-Mobile is configured under the APN.
  - RADIUS returns a Framed-Mask less than 32 bits.
  - The extra route comprises a network range of Framed-IP-Address + Framed-Mask.

  Workaround: Ensure that the RADIUS server is configured to return only a Framed-Mask of 32 bits.

Open Caveats—Cisco SAMI

This section lists the SAMI caveats that are open with Cisco IOS Release 12.4(22)YE.

- CSCsv82633

  On the Cisco SAMI, TTL processing/decrementing does not occur for IP packets.

  Workaround: There is no known workaround.

- CSCsy10472

  Under rare conditions, the Cisco SAMI PPC might encounter a fatal error during an image download/reload process, and display the following log at the PPC console:

  ```
  %PLATFORM-0-SAMI_INVALID_SLOT_ID: Invalid slot id 0 in ROMMON cookie at X
  ```

  followed by a traceback.

  This fatal error occurs during an image upgrade of a PPC, or a PPC reload sequence for any reason. The PPC starts up properly on subsequent reloads.

  Workaround: There is no known workaround.

Open Caveats—Other

This section lists additional caveats that are open and apply to Cisco IOS Release 12.4(22)YE.

- CSCsw87426

  cTap2StreamInterceptEnable cannot be set to True (enabled) unless a stream is added and set to active. However, when the stream is deleted, cTap2StreamInterceptEnable remains in a True state when it should be set to False (disabled), or alternatively, the True state should prevent the stream from being deleted.

  Workaround: There is no known workaround.

Resolved Caveats—Other

The following caveats are resolved in Cisco IOS Release 12.4(22)YE. This section describes only severity 1 and 2 caveats, and select severity 3 and 4 caveats.

- 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.

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 48
- Platform-Specific Documents, page 48
- Cisco IOS Software Documentation Set, page 48

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.4 and are located at 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 router documentation is available at:

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 guide. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference guide list 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 view a list of MIBs supported by Cisco, by product, go to: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Implementing GGSN Release 9.*x* on the Cisco SAMI

The following sections list related documentation (by category and then by task) to use when you implement a Cisco GGSN on the Cisco SAMI platform.

General Overview Documents

Core Cisco 7609 Router 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_roadmap09186a00801ebed9.html

Getting Started

- *Cisco 7600 Series Internet Router Essentials*

  http://cisco.com/en/US/products/hw/routers/ps368/products_quick_start09186a0080092248.html

- *Regulatory Compliance and Safety Information for the Cisco 7600 Series Internet Routers*

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/rcsi/index.html

Unpacking and installing the Cisco 7609 router:

- *Cisco 7609 Internet Router Installation Guide*

  http://cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_book09186a008007e036.html

Installing the Supervisor module and configuring the router (basic configuration, such as VLANs, IP):

- *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

Installing and completing the 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

Downloading the Cisco IOS software image containing GGSN feature set and configuring GGSNs on the SAMI:

- Cisco GGSN Release 9.0 Configuration Guide and Command Reference and Associated Release Notes for Cisco IOS Release 12.4(22)YE.

  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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the *Cisco GGSN Release 9.0 Configuration Guide* and the *Cisco GGSN Release 9.0 Command Reference* publications.