Release Notes for Cisco GGSN Release 10.*x* on the Cisco SAMI, Cisco IOS Software Release 12.4(24)YE Releases

Latest Publication Date: March 6, 2013, Cisco IOS Release 12.4(24)YE3e
Last Publication Date: January 9, 2012, Cisco IOS Release 12.4(24)YE3d

This release note describes the requirements, dependencies, and caveats for the Cisco Gateway General Packet Radio Service (GPRS) Support Node (GGSN) Release 10.*x*, Cisco IOS Release 12.4(24)YE releases 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(24)YE releases, see the "Caveats" section on page 16 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.

Note

- Cisco IOS Release 12.4(24)YE4 and later supports Cisco GGSN Release 10.2.
- Cisco IOS Release 12.4(24)YE3 to YE3e supports Cisco GGSN Release 10.1.
- Cisco IOS Release 12.4(24)YE toYE2 supports Cisco GGSN Release 10.0.

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(24)YE releases and includes the following sections:

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(24)YE Releases

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.124-24.YE*x*.bin	128	2	RAM

Hardware and Software Requirements

Implementing a Cisco GGSN Release 10.*x* 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 Mutlilayer 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(24)YE or later.

Note The Cisco GGSN Release 10.*x* software application ships preloaded on the Cisco SAMI and is automatically loaded onto each processor during an image upgrade. The Cisco GGSN Release 10.*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 PPC3 enter the **show version** EXEC command:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) SAMI Software (g8ik9s), Version 12.4(24)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

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 Cisco GGSN Release 10.*x*, note the following:

- The Cisco GGSN Release 8.0 and later 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, ensure that you configure the **no ip cef optimize neighbor resolution** command.

- 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
    ```

- 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 SAMI
IPv4	384,000
IPv6	48,000
PPP Regeneration	96,000
PPP	48,000

Table 3 Number of PDPs Supported in 2 GB SAMI

PDP Type	Maximum Number per SAMI
IPv4	816,000
IPv6	96,000
PPP Regeneration	192,000
PPP	96,000

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.

For implementation of a service-aware GGSN, the following additional important notes, limitations, and restrictions apply:

- You must enable RADIUS accounting between the CSG2 and GGSN to populate the Known User Entries Table (KUT) entries with the PDP context user information.
- You must configure CSG2 with the quota server address of the GGSN.
- Ensure that you configure service IDs on the CSG2 as numeric strings that match the category IDs on the Diameter Credit Control Application (DCCA) server.

- If you are not using RADIUS, ensure that you configure the Cisco CSG2 as a RADIUS endpoint on the GGSN.
- On the serving GRPS support node (SGSN), ensure that the value you configure for the number of GTP N3 requests and T3 retransmissions is 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 might impact slow TCP-based charging paths.

Single IP Cisco GGSN Usage Notes and Requirements

The following changes exist between the non-single IP Cisco GGSN and the single IP Cisco GGSN:

- Configuration

  The configuration of a single IP GGSN does not differ from a non-single IP GGSN. All configurations must be performed on the Proxy Control Processor (PCOP), which are then propagated to all Traffic and Control Plane processors (TCOPs). Failure of the command in any of the TCOPs causes a rollback of the configuration on the PCOP and other TCOPs.

  A few values configured on the PCOP, for example the maximum number of PDP contexts, are distributed to the TCOPs as seen in the following example:

```
sup-06-3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PPC3(config)#gprs maximum-pdp-context-allowed ?
  <5-4294967295>  Max PDP context allowed
PPC3(config)#gprs maximum-pdp-context-allowed 10000
PPC3(config)#end
PPC3#
PPC3#show run| i maximum-pdp-context-allowed
gprs maximum-pdp-context-allowed 10000
PPC3#execute-on all sh run | i maximum-pdp-context-allowed
gprs maximum-pdp-context-allowed 2000
gprs maximum-pdp-context-allowed 2000
gprs maximum-pdp-context-allowed 2000
gprs maximum-pdp-context-allowed 2000
gprs maximum-pdp-context-allowed 2000
PPC3#
```

- **show** Command Output Display

  The display of most **show** commands are aggregated to display consolidated outputs of all the TCOPs. However, a few **show** commands display the outputs from each TCOP.

  For example, the **show ip iscsi session** command displays output from all TCOPs:

```
PPC3#show ip iscsi session
----------- Slot 6/CPU 3, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
---------------------------------------------------------------
8         LINUX              Logged In            1
----------- Slot 6/CPU 4, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
---------------------------------------------------------------
7         LINUX              Logged In            1
----------- Slot 6/CPU 5, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
---------------------------------------------------------------
7         LINUX              Logged In            1
----------- Slot 6/CPU 6, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
---------------------------------------------------------------
7         LINUX              Logged In            1
----------- Slot 6/CPU 7, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
---------------------------------------------------------------
7         LINUX              Logged In            1
----------- Slot 6/CPU 8, show ip iscsi session -------------

ID        TARGET             STATE                CONNECTIONS
---------------------------------------------------------------
7         LINUX              Logged In            1
PPC3#
```

  Whereas, the **show gprs iscsi statistics** command aggregates the output from all TCOPs:

```
PPC3#show gprs iscsi statistics
GPRS iSCSI statistics for iSCSI Profile LINUX:
    Profile Name: LINUX
    Open Requests  = 5       ,    Failed Open Attempts  = 0
    Write Requests = 0       ,    Failed Write Requests = 0
    Read Requests  = 5       ,    Failed Read Requests  = 5
    Close Requests = 0       ,    Failed Close Requests = 0
    Number of DTRs in Write Queue = 0
    Number of DTRs in Read Queue = 0
PPC3#
```

- RADIUS

  For RADIUS responses to reach the correct TCOP, the following configuration on the Cisco GGSN is mandatory:

```
PPC3(config)#radius-server source-ports extended
```

- iSCSI
  a. The file systems for ISCSI storage is not visible on the PCOP. To view the file systems, execute the command on all TCOPs using the **execute-on all sh file systems** command:

```
PPC3#show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   snmp:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*     27740160      27736064     flash     rw   bootflash:
       131072        128947     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:

PPC3#execute-on all show file systems
----------- Slot 6/CPU 4, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   snmp:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*     27740160      27736064     flash     rw   bootflash:
       131072        129996     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
    3217522688    3217506304      disk     rw   sda0:#


----------- Slot 6/CPU 5, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   snmp:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*     27740160      27736064     flash     rw   bootflash:
       131072        129996     nvram     rw   nvram:
```

```
               -             -    opaque     wo   syslog:
               -             -   network     rw   rcp:
               -             -   network     rw   ftp:
               -             -   network     rw   http:
               -             -   network     rw   scp:
               -             -    opaque     ro   tar:
               -             -   network     rw   https:
               -             -    opaque     ro   cns:
    3217522688    3217506304      disk     rw   sda1:#


----------- Slot 6/CPU 6, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   snmp:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*     27740160      27736064     flash     rw   bootflash:
       131072        129996     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
    3217522688    3217506304      disk     rw   sda2:#


----------- Slot 6/CPU 7, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   snmp:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*     27740160      27736064     flash     rw   bootflash:
       131072        129996     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
    3217522688    3217506304      disk     rw   sda3:#


----------- Slot 6/CPU 8, show  file systems-------------

File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
```

```
              -             -    opaque     rw   archive:
              -             -    opaque     rw   system:
              -             -    opaque     rw   tmpsys:
              -             -   network     rw   snmp:
              -             -    opaque     rw   null:
              -             -   network     rw   tftp:
*     27740160      27736064     flash     rw   bootflash:
        131072        129996     nvram     rw   nvram:
              -             -    opaque     wo   syslog:
              -             -   network     rw   rcp:
              -             -   network     rw   ftp:
              -             -   network     rw   http:
              -             -   network     rw   scp:
              -             -    opaque     ro   tar:
              -             -   network     rw   https:
              -             -    opaque     ro   cns:
    3217522688    3217506304      disk     rw   sda4:#

PPC3#
```

b. To format ISCSI disks from the Cisco GGSN, establish a session with the TCOP and execute the **format** command:

```
sup#session slot 6 proc 4
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.64 ... Open

    ************************************************************
    **                  !!! WARNING !!!                       **
    **                                                        **
    **  You are accessing the Traffic Processor on this       **
    **  system. It is strongly advised to use the Control     **
    **  Processor (processor 3) for any activity.             **
    **                                                        **
    **  Please contact your Cisco Technical Support           **
    **  personnel for any support in using this interface.    **
    **                                                        **
    ************************************************************

06-3-4>en
06-3-4#
06-3-4#show sda0:
-#- --length-- -----date/time------ path
1            0 Feb 08 2010 16:50:54 root
2           64 Feb 08 2010 16:50:58 root/master.dat
3            0 Feb 08 2010 16:50:56 salvage

3217506304 bytes available (16384 bytes used)

06-3-4#format sda0:
Format operation may take a while. Continue?
Format operation will destroy all data in "sda0:".  Continue? Writing Monlib
sectors..
Monlib write complete

Format: All system sectors written. OK...

Format: Total sectors in formatted partition: 6296544
Format: Total bytes in formatted partition: 3223830528
Format: Operation completed successfully.

Format of sda0: complete
06-3-4#
```

```
SAMI 6/4: Feb 24 06:36:07.129: %RSM-3-WARNING: Warning: iSCSI target in profile
LINUX cannot be used for storing/retrieving CDRs. Disk is formatted. Please
disconnect and connect to the Target.
```

- Configuration locking

  If any debug error messages such as “Configuration in progress. Dropping the create PDP req. Please try later!” or “APN in config lock and disallows new create” is observed, verify the configure-related PDP creation blocking using the following command in privilege EXEC mode:

```
Router#show gprs configuration-lock counter

 system level lock counter: 0
 access point 1 apn1 counter:0
 access point 2 apn2 counter:0
```

  This command displays GGSN configuration locking counters. There are two kinds of configuration locking counters, system level locking counters and access-point locking counters. If the system level locking counter is non-zero, any create PDP context requests are blocked. If one access-point locking counter is non-zero, any create PDP context requests referred to that access point are blocked. Typically these counters are zero and a non-zero state is transient. However, if a user observes a configuration-lock counter remains in a non-zero state, use the following command to reset all of the configuration lock counters to zero.

```
Router# clear gprs configuration-lock counter
```

  A warning message displays if there is non-zero counter.

New and Changed Information

The following sections list the new features or changed behavior in the Cisco IOS Release 12.4(24) YE releases. Releases note listed do not contain new features or changed behavior.

- New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE7, page 13
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE6, page 16
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE4, page 17
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE3e, page 17
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE3b, page 19
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE3, page 20
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE2, page 21
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE1, page 21
- New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE, page 23

For detailed information about the new and existing features in GGSN Release 10.*x*, Cisco IOS Release 12.4(24) YE releases, refer to the *Cisco GGSN Release 10.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(24)YE7

The following features are introduced with or incorporated in Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE7:

Automatic Stuck PDP Context Identification and Removal

Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE7 incorporates the support for automatic identification and removal of PDP contexts that are stuck in either the creation or deletion process, which was introduced in Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3b.

By default, this background process runs automatically every 15 minutes on the active GGSN in a redundant configuration. The process detects and notifies you of stuck PDPs. Optionally, you can configure the GGSN to automatically clear the stuck PDPs, or you can manually clear them.

Enabling the Automatic Detection and Clearing of Stuck PDPs

To configure the automatic identification, and optionally removal of stuck PDP contexts, complete the following task in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp pdp-context timeout stuck-pdp [threshold | disable]`	Enables automatic detection of stuck PDP contexts and the generation of syslog notifications. By default, automatic detection and notification is enabled. Optionally, specify: • *threshold*—(Optional) Configures the GGSN to automatically clear PDPs stuck in a creation or deletion process longer than the *threshold* value you specify, in minutes. A valid value is a number between 15 and 1440. The default is 15 minutes. • **disable**—Disables automatic detection and clearing of stuck PDPs.

The following is an example of a syslog message sent when a stuck PDP is detected:

```
SAMI 4/4: Sep  5 04:55:20.750: %GPRSFLTMG-4-GTP_PDP_STUCK: GSN: 110.50.0.50, TEID:
1122330000001211, APN: eggsn_postpaid,MSISDN: 112323000000121, Reason : 2, flags: 4C0091
```

Manually clearing Stuck PDPs

Before manually clearing a stuck PDP, you must place the associated access point in maintenance mode by using the **service-mode maintenance** command in access-point configuration mode. Once you have cleared the command, place the access point back in operational mode by using the **service-mode operational** command in access-point configuration mode.

To manually clear a stuck PDP by Tunnel Identifier (TID) on the active GGSN, complete the following task in privilege EXEC mode.

Command	Purpose
`Router# clear gprs gtp pdp-context access-point index force tid`	Clears the stuck PDP by TID on the active GGSN.

Note Clearing the stuck PDP on the active GGSN should remove the same PDP on the standby GGSN. However, if for some reason the PDP is not removed on the standby GGSN when it is cleared on the active GGSN, use the **clear gprs gtp pdp-context tid** *tid* command in privileged EXEC mode on the standby GGSN to manually remove it.

Gy Interface Enhancement for Standalone Prepaid Subscribers

With Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE7, you can configure the Cisco GGSN to create a PDP context and send a Credit-Control-Request (CCR-U) that includes either a configured Service-Identifier or the APN index number as the Service-Identifier when it receives a Credit-Control-Answer (CCA-I) from an Online Charging System (OCS), which does not contain a Service-Identifier.

Before enabling the Service-Identifier Gy interface enhancement, note the following:

- Support for service-aware billing must be enabled on the GGSN by using the **gprs service-aware** command in global configuration mode.
- The Cisco GGSN must be configured to perform prepaid quota enforcement in standalone mode by using the **gprs prepaid stand-alone** command in global configuration mode.
- Specify only numeric values for the **service-id** *string* as defined by 3GPP 32.299 V7.7.0.
- You must place an APN in maintenance mode by using the **service-mode maintenance** command in access-point configuration mode before configuring or unconfiguring the **service-id** command.
- You cannot configure the **service-id** command under a virtual APN.
- You cannot use the **service-id** command for enhanced GGSN (eGGSN) calls.

To configure the GGSN to send a CCR-U that includes a Service-Identifier or an APN index ID as a Service-Identifier when it receives a CCA-I from the OCS that does not include a service ID, use the following command while in access-point configuration mode:

Command	Purpose
`Router(config-access-point)# service-id [default | numeric-string]`	Configures the GGSN to send a Service-Identifier or the APN index as the Service-Identifier in the CCR-U when it receives a CCA-I that does not contain a Service-Identifier, where: • **default**—Configures the GGSN to use the APN index as the Service-Identifier. • *numeric-string*—Configures the GGSN to use the specified numeric string or range as the Service-Identifier. A valid value is a number between 1 and 65535.

Throttling GTP Request Re-Enqueues

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MIB Changes

In Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE7 and later, the GetNext and GetBulk requests are disabled for the GGSN Subscriber table (cGgsnExtSubscriberTable) in the CISCO-GGSN-EXT-MIB.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE6

Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE6 introduces support for the **diameter vendor supported 3gpp** command **always** keyword option.

When enabling support for a Third-Generation Partnership Project (3GPP) Gy-compliant Diameter Credit Control Application (DCCA) implementation, when the Diameter peer advertises that it supports 3GPP during the capability exchange between the GGSN and the Diameter peer, you must configure the following commands:

- **gprs dcca 3gpp**—Configures the GGSN to send 3GPP Vendor Specific Attributes (VSAs) in DCCA messages to the Diameter server.
- **diameter vendor supported 3gpp**—Configures the Diameter server to advertise support for the 3GPP AVPs.

However, if the Diameter server (also known as the Online Charging System [OCS]) supports 3GPP but does not negotiate 3GPP in the capability exchange, you must configure the following commands to ensure that the GGSN sends 3GPP AVPs even when the Diameter server does not advertise 3GPP support:

- **gprs dcca 3gpp**
- **diameter vendor supported 3gpp always**.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE4

Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE4 introduces support for the following:

- Credit-Control-Failure-Handling (CCFH) vendor-specific attribute value pair (AVP) tuning for prepaid and postpaid subscribers.

  By default, when service-aware billing is implemented on the Cisco GGSN using a Diameter Credit Control Application, the Cisco GGSN receives a Diameter Credit-Control-Answer (CCA) and applies it uniformly for both prepaid and postpaid subscribers.

  With Cisco GGSN Release 10.2 and later, you can associate up to 16 charging profiles with different subscribers in an APN. The ability to associate multiple charging profiles with different subscribers in an APN enables operators to customize the CCFH for both prepaid and postpaid subscribers. The CCFH determines how the GGSN behaves if a CCA failure occurs.

- Diameter Credit Control Application (DCCA) Credit Control Requests (CCRs) enhancements:
  - Support for grouping message-level AVPs under the Packet Switched Information (PS-Information) AVP.
  - Support for grouping the International Mobile Subscriber Identity (IMSI) AVP under the Subscription-ID AVP.
  - Support for the following new AVPs:

    The International Mobile Equipment Identity (IMEI) in the User-Equipment-Info AVP (group level)

    3GPP-SGSN-MCC-MNC AVP (message level)

    3GPP-MS-Timezone AVP (message level)
- Delayed quota reauthorization for DCCA subscribers.

For information about each of these features, see the *Cisco GGSN Release 10.2 Configuration Guide*.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE3e

Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3e includes the following **show** command enhancements:

- The **show tech** command has been enhanced to also display the output of **show sctp** commands. (CSCue48147)
- The **show gprs gtp statistics** command and **show gprs access-point statistics all** command have been enhanced to include the number of update PDP context requests received in the command output as seen in the fields displayed in **bold** in the following command output:

```
GGSN#sh gprs gtp statistics
GPRS GTP Statistics:
  version_not_support        0           msg_too_short              0
  unknown_msg                0           unexpected_sig_msg         0
  unexpected_data_msg        0           unsupported_comp_exthdr    0
  mandatory_ie_missing       0           mandatory_ie_incorrect     0
  optional_ie_invalid        0           ie_unknown                 0
  ie_out_of_order            0           ie_unexpected              0
  ie_duplicated              0           optional_ie_incorrect      0
  pdp_activation_rejected    0           tft_semantic_error         0
  tft_syntactic_error        0           pkt_ftr_semantic_error     0
```

```
  pkt_ftr_syntactic_error    0            pdp_wo_tft_exist           0
  non_existent               1            path_failure               0
  total_dropped              0            signalling_msg_dropped     0
  data_msg_dropped           0            no_resource                0
  get_pak_buffer_failure     0            rcv_signalling_msg         1
  snd_signalling_msg         1            rcv_pdu_msg                0
  snd_pdu_msg                0            rcv_pdu_bytes              0
  snd_pdu_bytes              0            total created_pdp          0
  total deleted_pdp          0            total created_sec_pdp      0
  total deleted_sec pdp      0            total created_ppp_pdp      0
  total deleted stuck pdp    0            total stuck pdp            0
  total deleted_ppp_pdp      0            total MSinit pdp update    1
  ppp_regen_pending          0            ppp_regen_pending_peak     0
  ppp_regen_total_drop       0            ppp_regen_no_resource      0
   ntwk_init_pdp_act_rej      0           total ntwkInit created pdp 0
   single pdp-session cleared 0           total ntwkInit update pdp  0
   total update responses rcv 0           total COA msg received     0
   total COA msgs discarded   0           total COA triggered update 0
   total err indications rcvd 0           total err indications sent 0
   Number of times DT enabled 0           total EI rcvd on DT PDPs   0
   total update fail DT pdps  0           msg dropped on config      0
   invalid_tid_in_pdp         0           invalid_tid_in_pak         0
   pdp dropped invalid sigmsg 0           invalid_tid_in_pak         0
   pdp dropped invalid sigmsg 0
  created ipv6 pdp           0            rejected ipv6 pdp          0
  deleted ipv6 pdp           0            created ipv6 pdpmcb        0
  deleted ipv6 pdpmcb        0
  rcvd ipv6 pdu              0            sent ipv6 pdu              0
  rcvd ipv6 data bytes       0            sent ipv6 data bytes       0
  newinfo acct recs queued   0            newinfo acct recs failed   0
Debug info:
  path_fail_local_del_pdp    0            ver_upgrade_local_del      0
  no_sgsn_local_del_pdp      0            ver_fallback_local_del     0
  no_wait_sgsn_local_del_pdp 0            no_req_sgsn_local_del_pdp  0
  create_collide_with_delete 0            version_changes            0
  rcv_retransmit_create_req  0            create_as_update           0
GGSN#

GGSN#sh gprs access-point statistics 3
    PDP activation intiated by MS:                      0
    Successful PDP activation intiated by MS:           0
    Total secondary PDPs created:                       0
    Total secondary PDPs deleted:                       0
    Total Stuck pdp                                     0
    Total Stuck pdp deleted                             0
    Dynamic PDP activation initiated by MS:             0
    Successful dynamic activation initiated by MS:      0
    PDP update initiated by MS:                         0
    Successful PDP update initiated by MS:              0
    PDP deactivation initiated by MS:                   0
    Successful PDP deactivation initiated by MS:        0
    Network initiated PDP activation:                   0
    Successful network initiated PDP activation:        0
    PDP deactivation initiated by GGSN:                 0
    Successful PDP deactivation initiated by GGSN:      0
    PDP update initiated by GGSN:                       0
    Successful PDP update initiated by GGSN:            0
    upstream data volume in octets:                     0
    downstream data volume in octets:                   0
    upstream packet count:                          0
    downstream packet count:                        0
    DHCP address requests sent by GGSN:             0
    DHCP address requests successful:               0
    DHCP address release sent by GGSN:              0
```

```
    Total number of COA requests received:          0
    Total number of successful COA requests:        0
    Number of times direct tunnel enabled:          0
GGSN#
```

(CSCue57186)

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE3b

The following new features supported in Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3b:

- Automatic Stuck PDP Context Identification and Removal, page 13
- Throttling GTP Request Re-Enqueues, page 15.

Enabling the Automatic Detection and Clearing of Stuck PDPs

To configure the automatic identification, and optionally removal of stuck PDP contexts, complete the following task in global configuration mode:

Command	Purpose
`Router(config)# gprs gtp pdp-context timeout stuck-pdp [threshold | disable]`	Enables automatic detection of stuck PDP contexts and the generation of syslog notifications. By default, automatic detection and notification is enabled. Optionally, specify: • *threshold*—(Optional) Configures the GGSN to automatically clear PDPs stuck in a creation or deletion process longer than the *threshold* value you specify, in minutes. A valid value is a number between 15 and 1440. The default is 15 minutes. • **disable**—Disables automatic detection and clearing of stuck PDPs.

The following is an example of a syslog message sent when a stuck PDP is detected:

```
SAMI 4/4: Sep  5 04:55:20.750: %GPRSFLTMG-4-GTP_PDP_STUCK: GSN: 110.50.0.50, TEID:
1122330000001211, APN: eggsn_postpaid,MSISDN: 112323000000121, Reason : 2, flags: 4C0091
```

Manually clearing Stuck PDPs

Before manually clearing a stuck PDP, you must place the associated access point in maintenance mode by using the **service-mode maintenance** command in access-point configuration mode. Once you have cleared the command, place the access point back in operational mode by using the **service-mode operational** command in access-point configuration mode.

To manually clear a stuck PDP by Tunnel Identifier (TID) on the active GGSN, complete the following task in privilege EXEC mode.

Command	Purpose
`Router#` **`clear gprs gtp pdp-context access-point`** *`index`* **`force`** *`tid`*	Clears the stuck PDP by TID on the active GGSN.

Note Clearing the stuck PDP on the active GGSN should remove the same PDP on the standby GGSN. However, if for some reason the PDP is not removed on the standby GGSN when it is cleared on the active GGSN, use the **clear gprs gtp pdp-context tid** *tid* command in privileged EXEC mode on the standby GGSN to manually remove it.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE3

Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3 introduces support for RADIUS Controlled Redirection.

The RADIUS Controlled HTTP Redirection feature enables the Cisco GGSN to redirect the HTTP traffic of subscribers to an Advice-of-Charge (AoC) page that notifies them of new tariff changes when they are roaming in a foreign PLMN.

For information about configuring RADIUS controlled HTTP redirection, see the *Cisco GGSN Release 10.1 Configuration Guide*.

Additionally, in Cisco IOS Release 12.4(24)YE3, the **ip** keyword option was dropped from the syntax of the **redirect all ip** access-point configuration command.

Note The **ip** keyword option was added back to the **redirect all ip** command syntax in Cisco IOS Release 12.4(24)YE4.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE2

The following enhancements and features are introduced in Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE2.

- Overlapping Local IP Address Pools

  Support for the Overlapping Local IP Address Pools feature is introduced in Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE2.

  The Overlapping Local IP Address Pools feature improves flexibility in assigning IP addresses dynamically. This feature allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

  For information about configuring overlapping local IP address pools, see the *Cisco GGSN Release 10.0 Configuration Guide*.

- Support for the **copy** command on the TCOPs (reference CSCti68023)

  Cisco IOS Release 10.0, Cisco IOS Release 12.4(24)YE2 supports the **copy** command as a method of retrieving CDRs written to an iSCSI device in a single IP environment.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE1

The following new implementations and behavior changes exist in this release of the Cisco GGSN:

- Authentication, Authorization, and Accounting Enhancements, page 13
- Internet Small Computer System Interface Enhancements, page 14
- MIB Updates, page 14

Authentication, Authorization, and Accounting Enhancements

With Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE1, support for private Authentication, Authorization, and Accounting (AAA) server groups is introduced using existing CISCO-AAA-SERVER-MIB objects.

This support resolves CSCtg65556.

Internet Small Computer System Interface Enhancements

The following Internet Small Computer System Interface (iSCSI) enhancements are introduced in Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE1.

- 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.

For detailed information about these new commands, see the *Cisco GGSN Release 10.0 Configuration Guide*.

MIB Updates

The following MIB files have been updated to support the following Cisco GGSN Release 10.0 features:

- CSG load balancing
  - CISCO-GPRS-ACC-PT-MIB
  - CISCO-GGSN-SERVICE-AWARE-MIB
- Enhanced CDRs
  - CISCO-GPRS-ACC-PT-MIB
  - CISCO-GGSN-SERVICE-AWARE-MIB
  - CISCO-GGSN-EXT-MIB
- Geographical Redundancy
  - CISCO-GGSN-GEO-MIB
  - CISCO-HSRP-EXT-MIB
- Granular Charging
  - CISCO-GPRS-CHARGING-MIB
  - CISCO-GTP-MIB
- GRX Traffic Segregation
  - CISCO-GGSN-MIB
- OCS load balancing
  - CISCO-GPRS-CHARGING-MIB

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE

The following new implementations and behavior changes exist in this release of the Cisco GGSN:

- Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE introduces support for the following features:
  - Single IP operation and management of the Cisco SAMI

    Cisco GGSN Release 10.0 and later supports a single IP architecture. The single IP architecture enables all six Cisco GGSN instances running on the Cisco SAMI processors to function as one Cisco GGSN instance.

    For single IP usage notes, see "Single IP Cisco GGSN Usage Notes and Requirements" section on page 7.
  - Enhanced prepaid subscriber features

    - Dynamic HTTP redirection and termination with Final Unit Indication (FUI)

    - Activity-based time billing—Activity-based billing, as defined in 3GPP, bills users for only the periods of on the network that activity is occurring, instead of billing them for the entire time they are logged on the network.
  - Dynamic IP address management

    With Release 10.0 and later, the Cisco GGSN supports dynamic IP address allocation. Dynamic IP address allocation enables operators to implement a Cisco GGSN without subnetting requirements. The Cisco GGSN supports dynamic IP address allocation from DHCP, RADIUS, and local pools.
  - Cisco CSG2 load balancing

    With the advent of a single IP architecture of Cisco GGSN Release 10.0 and later, the Cisco GGSN quota server interface supports multiple Cisco CSG2s. Service-aware users from the Cisco GGSN are load-balanced among the Cisco CSG2s.
  - OCS load balancing

    In earlier releases of the Cisco GGSN, you could configure only one DCCA server at a time per APN, but you could configure different DCCA servers for the same APN on the GGSN instances on the Cisco SAMI.

    With the transition to a single IP architecture in Cisco GGSN Release 10.0, the separate GGSN instances running on the six Cisco SAMI processors function as a single GGSN, rather than six GGSNs. To enable an APN to communicate with multiple DCCA servers, with Cisco GGSN Release 10.0 and later, you can configure multiple DCCA profiles under a charging profile applied to an APN.

For more information about the features introduced in Cisco GGSN Release 10.0, see the *Cisco GGSN Release 10.0 Configuration Guide*.

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(24)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(24)YE7

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE7 image:

Open Caveats

Note Caveats that are open in the most current 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 25
- Cisco SAMI Open Caveats, page 26
- Miscellaneous Open Caveats, page 26

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)YE7:

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtr22870

  When PPP PDP type sessions are created, the transmit and receive counters displayed by using the the **show gprs gtp pdp** privileged EXEC command continuously increase even without traffic. The counters are getting incremented due to PPP LCP echo requests and responses.

  This condition occurs only with PPP PDP type subscribers from Cisco IOS Release 12.4(24)YE4 and later.

  Workaround: There is currently no known workaround.

- CSCtt25749

  A mismatch between the "InUse" counters in the **show ip local pool** command output between an active and standby GGSN might occur. The counters of the standby GGSN might display more IPs in use than the counters of the active GGSN.

  This condition occurs on the standby Proxy Control Processor (PCOP) when it could not free an IP address under certain rare circumstances.

  Workaround: There is currently no known workaround, however, this condition does not impact the standby GGSN because the actual IP allocation occurs from the Traffic Control Processors (TCOPs) of the standby GGSN.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE7:

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 and later single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

```
sup#delete sami#7-fs:core/*.*
Delete filename [core/*.*]?
Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

  Workaround: There is currently no known workaround.

Miscellaneous Open Caveats

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE7:

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE7. Only severity 1 and 2 caveats and select severity 3 caveats are listed

Cisco GGSN Resolved Caveats

This section lists GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(24)YE7.

- CSCto88380

  Even with charging characteristics reject configured (by using the **gprs charging characteristics reject** global configuration command), the GGSN selects the default charging profile for an unmatched charging characteristic value instead of sending a negative response to the SGSN as designed.

  This condition occurs when the GGSN is configured to reject Create PDP Context requests for which no charging profile can be selected.

- CSCtq15071

  When the Diameter Credit Control Application (DCCA) server is down, and the Credit-Control-Fault-Handling (CCFH) action is set to default (terminate), PDP sessions are being converted to postpaid sessions instead of being terminated.

- CSCtr22435

  When a new APN with charging characteristics is unconfigured, a traceback occurs.

  This condition occurs when a new access point is configured with charging characteristics, and then the access point is unconfigured.

- CSCtr22984

  An SNMP walk for AAA-SERVER-MIB causes delayed **show** and configuration commands and delayed responses to SNMP polls.

  This condition occurs when RADIUS is configured with more than 30 server entries using the following command:

  radius-server host *ip addr* **auth-port 1645 acct-port 1646**

- CSCtr31369

  A GTPv0 create request over an existing GTPv1 PDP causes a high CPU.

  This condition occurs only when the existing GTPv1 PDP is waiting for the completion of an update request and then a GTPv0 create is initiated.

  (CSCtr31369 and CSCtr30916 fix the symptom and free the CPU by dropping the new GTPv0 create request.)

- CSCtr42950 (duplicate of CSCtr56632)

  The Cisco GGSN might arrive in a situation in which the CPU on certain Traffic and Control Plane processors (TCOPs) reaches almost 100%. When this condition occurs, stuck PDP sessions are also seen on the affected TCOPs.

  This condition causes subscribers to experience problems in the GTP control path (for example, setting up PDP sessions) and in the data path (for example, sending data through the PDP session). This condition typically occurs in a service-aware implementation and appears to begin when the GGSN assumes a path restart has occurred, which indicates that the SGSN is restarting, when in fact, that is not the case.

- CSCtr56558

  When a very high number of GTPv0 and GTPv1 users handoff from one SGSN to another, the following error message with a traceback might be seen and could possibly lead to a reload of the standby GGSN.

  ```
  IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0)
  ```

  This condition could occur when a very high number of GTPv0 and GTPv1 users handoff from one SGSN to another at the same time at a very high rate.

- CSCtr61654

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

- CSCtr87690

  The GGSN does not create PDPs even when there is sufficient IP address space. The RefCount in the International Mobile Subscriber Identity (IMSI) sticky database is negative one (-1).

  ```
  GGSN#show sami sm imsi
  IMSI: 214350000000001, Permanent: NO,  Location: 7
    MSISDN: 91214365060000000F100  Length:9
  4u87efCount:-1, version:1, SeqNum:2, NSAPI_MAP:0000
  IMSI: 214350000000002, Permanent: NO,  Location: 4
    MSISDN: 91214365060000000F200  Length:9
    RefCount:-1, version:1, SeqNum:2, NSAPI_MAP:0000
  ```

  This condition occurs with a single IP architecture (Proxy Control Processor [PCOP] and Traffic and Control Plane processors [TCOP]) when all the IP addresses in a TCOP are “In Use” and the TCOP attempts a reassignment. The PCOP fails to reassign the session because of the RefCount -1.

- CSCtr90135

  “91” is added to the “calling-number” AVP in Incoming-Call-Request (ICRQ) messages even when the **no gprs radius msisdn first-byte** global configuration command is configured.

- CSCtr90757

  The GGSN retransmits a lot of RADIUS Accounting Start requests for postpaid subscribers. The current behavior is as follows:

  a. The GGSN sends a RADIUS Accounting Start.

  b. The Cisco Content Services Gateway-2nd Generation (CSG2) sends a Gx Diameter Credit Control Request (CCR-I) to the Policy Control and Charging Rules Function (PCRF).

  c. The PCRF sends a Credit Control Answer (CCA-I) with either a 4001 or 5003 result code.

  d. The CSG2 sends a RADIUS Change of Operation (CoA) with AUTH_FAILED (0x02).

  e. The GGSN acknowledges the CoA but retransmits the Accounting Start, causing a lot of retransmission until the RADIUS times out.

  In this scenario, the GGSN relies on the RADIUS timeout and the signaling impacts the network.

  The desired behavior is for the GGSN to not retransmit the RADIUS Accounting Start request after receiving a CoA with Auth_failed but instead send a Create PDP Context Deny.

  This condition occurs with postpaid subscribers, whom are not allowed to use the Gx PCRF.

- CSCtr93403

  The following syslog message appears intermittently on the GGSN:

  ```
  GPRSFLTMG-4-CHARGING: GSN: 0.0.0.0, TID: 0000000000000000, APN: NULL, Reason: 13,
  Trying to close a NULL cdr_entry
  ```

  This condition occurs even when the charging function is not configured.

- CSCts05678

  There is a mismatch of the local IP address pool “In Use” count between the Proxy Control Processor (PCOP) and Traffic and Control Plane processors (TCOP). This occurs because some of the IP address in the PCOP are not freed even though the PDP context is cleared.

  For example:

  ```
  GGSN#show gprs gtp status
  GPRS GTP Status:
    activated gtpv0 pdp     0
    activated gtpv1 pdp     0
    activated ms            0
    activated ipv6 ms       0
    activated gtpv0 v6 pdp  0
    activated gtpv1 v6 pdp  0
    activated ppp regen pdp 0
    activated ppp pdp       0
    gtp's va hwidbs         0
    gtp's va swidbs         0
    gtp ipv6 swidbs         0
    gtp direct tunnel PDPs  0
  Service-aware Status:
    Prepaid PDPs            0
    Postpaid PDPs           0
  IST-GGSN-07#sh ip lo
  IST-GGSN-07#sh ip local poo
  IST-GGSN-07#sh ip local pool

  Pool                    Begin           End             Free  In use   Blocked
  ** pool <internet> is in group <internet>
  internet                178.241.128.0   178.241.255.255 32744      24       0
                           188.57.192.0    188.57.255.255  16373      11       0
                           188.58.96.1     188.58.127.255  8184       7        0
  ```

```
                          31.142.96.0     31.142.127.255  8188        4        0
** pool <wap> is in group <wap>
wap                     10.51.0.1       10.51.254.255   64798     481        0
** pool <mgb> is in group <mgb>
mgb                     188.59.176.1    188.59.191.255  4095        0        0
** pool <streaming> is in group <streaming>
streaming               10.52.80.1      10.52.87.255    2044        3        0
** pool <test15> is in group <test15>
test15                  31.142.96.0     31.142.127.255  8192        0        0
```

- CSCts23411

  Sometimes, the tunnel identifier (TID) value in a GTPv0 create PDP context response is corrupt. This condition occurs with roaming subscribers.

- CSCts74384

  For PPP-Regen users, the Time to Live (TTL) value of the IP packet in the downstream direction (from L2TP network server [LNS] to mobile subscriber [MS]), is decremented by 1, whereas in the upstream direction (from MS to LNS server), the TTL value is not decremented.

  This condition occurs only for PPP-Regen users.

- CSCts79810

  Input errors are seen on Cisco GGSN Traffic and Control Plane processors (TCOPs) with specific traffic patterns and signaling.

  This condition occurs when the idle timeout value is configured to a low value (300 seconds). When the idle timeout value is configured to a higher value (for example, 3600 or 7200 seconds), the input errors are not seen.

- CSCts87714

  3GPP-Selection-Mode (12) is not added under Packet Switched Information (PS-Information) AVP, even though the **gprs dcca avp grouped ps-information** global configuration command is configured.

- CSCtt16267

  The Cisco SAMI might crash when connecting to the charging gateway.

  This condition might occur when the charging gateway is connected to the GGSN, if the GGSN receives a different restart counter (recover information element [IE]) value from the charging gateway. Additionally, any pending call detail records (CDRs) in the GGSN could potentially lead to a crash.

- CSCtt33848

  A timing issue between a PDP deletion and a Diameter Credit Control Application (DCCA) response causes the Cisco SAMI to crash.

  This condition occurs only for a standalone prepaid user, and only if the GGSN receives a protocol error response from DCCA during the deletion of a prepaid PDP.

Cisco SAMI Resolved Caveats

This section lists a Cisco SAMI caveat that is resolved with Cisco IOS Release 12.4(24)YE7.

- CSCtc95114

  When performing a write memory or copying a file to the bootflash of a PowerPC (PPC), the Cisco SAMI drops a few packets.

- CSCtq42221

  When the Cisco IOS Software image is loaded, the counter for gig 0/0 starts incrementing. If there is no traffic on the router, the input queue drops and continues to increment.

- CSCts68928

  A configuration download error occurs with the following message:

  ```
  %IPC-0-CFG_DOWNLOAD_ERROR: Configuration download/parse error: Failed to download
  config on one or more processors, traffic will get blocked -Process= "Init", ipl= 0,
  pid= 3
  ```

  This condition occurs when the erase bootflash command is issued on the PCOP.

Miscellaneous Resolved Caveat

This section lists the miscellaneous caveats that are resolved with Cisco IOS Release Cisco IOS Release 12.4(24)YE7.

- CSCte89022

  Gateway might reload while handling a Virtual Private Dialup Network (VPDN) call due to invalid memory reference.

- CSCtb39102

  In a redundant implementation, a session is not synchronized to a standby unit if the MTU of the Gigabit0/0 interface of the active SAMI is set to1600 bytes. The router could also perform a redundancy framework (RF) self-reload.

- CSCtj87180

  A Layer 2 Tunneling Protocol Access Concentrator (LAC) router running Virtual Private Dialup Network (VPDN) might crash when it receives an invalid redirect from a peer with a of “SSS Manager Disconnected Session” Call-Disconnect-Notify (CDN) error message.

  This symptom is observed when the LAC router receives an the following message from the multihop peer:

  ```
  Error code(9): Try another directed and Optional msg: SSS Manager disconnected session
  <<<< INVALID
  ```

- CSCtl48268

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

Caveats - Cisco IOS Release 12.4(24)YE6

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE6 image:

Open Caveats

Note Caveats that are open in the most current 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

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)YE6:

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtn49917

  When the RADIUS Controlled Redirection feature is enabled, when a prepaid subscriber is converted to a postpaid subscriber, the conversion is not synchronized to the standby GGSN. In the standby GGSN, the subscriber continues to be a postpaid user only.

  This condition occurs only when RADIUS Controlled Redirection is enabled when running Cisco IOS Release 12.4(24)YE3.

  Workaround: Disable the RADIUS Controlled Redirection feature.

- CSCto88380

  Even with charging characteristics reject configured (by using the **gprs charging characteristics reject** global configuration command), the GGSN selects the default charging profile for an unmatched charging characteristic value instead of sending a negative response to the SGSN as designed.

  This condition occurs when the GGSN is configured to reject Create PDP Context requests for which no charging profile can be selected.

  Workaround: There is currently no known workaround.

- CSCtq15071

  When the Diameter Credit Control Application (DCCA) server is down, and the Credit-Control-Fault-Handling (CCFH) action is set to default (terminate), PDP sessions are being converted to postpaid sessions instead of being terminated.

  Workaround: There is currently no known workaround.

- CSCtr22435

  When a new APN with charging characteristics is unconfigured, a traceback occurs.

  This condition occurs when a new access point is configured with charging characteristics, and then the access point is unconfigured.

  Workaround: There is currently no known workaround.

- CSCtr22870

  When PPP PDP type sessions are created, the transmit and receive counters displayed by using the the **show gprs gtp pdp** privileged EXEC command continuously increase even without traffic. The counters are getting incremented due to PPP LCP echo requests and responses.

  This condition occurs only with PPP PDP type subscribers from Cisco IOS Release 12.4(24)YE4 and later.

  Workaround: There is currently no known workaround.

- CSCtr42950

  The Cisco GGSN might arrive in a situation in which the CPU on certain Traffic and Control Plane processors (TCOPs) reaches almost 100%. When this condition occurs, stuck PDP sessions are also seen on the affected TCOPs.

  This condition causes subscribers to experience problems in the GTP control path (for example, setting up PDP sessions) and in the data path (for example, sending data through the PDP session). This condition typically occurs in a service-aware implementation and appears to begin when the GGSN assumes a path restart has occurred, which indicates that the SGSN is restarting, when in fact, that is not the case.

  Workaround: Restart or failover the Cisco GGSN.

- CSCtr56558

  When a very high number of GTPv0 and GTPv1 users handoff from one SGSN to another, the following error message with a traceback might be seen and could possibly lead to a reload of the standby GGSN.

  ```
  IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0)
  ```

  This condition could occur when a very high number of GTPv0 and GTPv1 users handoff from one SGSN to another at the same time at a very high rate.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE6:

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 and later single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

  ```
  sup#delete sami#7-fs:core/*.*
  Delete filename [core/*.*]?
  Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
  ```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

  Workaround: There is currently no known workaround.

- Miscellaneous Open Caveats

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE6:

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE6. Only severity 1 and 2 caveats and select severity 3 caveats are listed

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

Cisco GGSN Resolved Caveats

This section lists GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(24)YE6.

- CSCso02147

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCth11006

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCti48483

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCtj04672

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCtr09665

  When a non existent or failed Diameter server is configured on the Cisco GGSN, it might exhaust all available sockets for Diameter communication.

- CSCtq56946

  The Cisco GGSN does not send 3GPP attribute-value pair (AVPs) to the Diameter peer even when the **gprs dcca 3gpp** global configuration command is configured.

  This condition occurs if the Diameter peer does not negotiate the capability as 3GPP in the Capability Exchange Answer (CEA) message. If this occurs, the GGSN does not send the 3GPP AVPs.

  For more information about this fix, see the "New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE6" section on page 16.

- 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.

- CSCtr61828

  The Cisco GGSN always sends the default Dynamic Feedback Protocol (DFP) weight of 8 to the Cisco IOS SLB on the supervisor regardless of the weight dynamically reported by the individual Traffic and Control Plane processors (TCOPs).

- CSCtr66659

  The Cisco GGSN load balancer state becomes stuck in a DFP_THROTTLED state when the maximum number of PDPs are created, and it is unable to exit from this state when the number of PDPs decreases. This condition occurs when GGSN is reporting dynamic weights to a Dynamic Feedback Protocol (DFP) manager like GTP SLB.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)YE6.

Caveats - Cisco IOS Release 12.4(24)YE5

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE5 image:

- Open Caveats, page 16
- Resolved Caveats, page 19

Open Caveats

Note Caveats that are open in the most current 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 17
- Cisco SAMI Open Caveats, page 19
- 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(24)YE5:

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtn49917

  When the RADIUS Controlled Redirection feature is enabled, when a prepaid subscriber is converted to a postpaid subscriber, the conversion is not synchronized to the standby GGSN. In the standby GGSN, the subscriber continues to be a postpaid user only.

  This condition occurs only when RADIUS Controlled Redirection is enabled when running Cisco IOS Release 12.4(24)YE3.

  Workaround: Disable the RADIUS Controlled Redirection feature.

- CSCto88380

  Even with charging characteristics reject configured (by using the **gprs charging characteristics reject** global configuration command), the GGSN selects the default charging profile for an unmatched charging characteristic value instead of sending a negative response to the SGSN as designed.

  This condition occurs when the GGSN is configured to reject Create PDP Context requests for which no charging profile can be selected.

  Workaround: There is currently no known workaround.

- CSCtq15071

  When the Diameter Credit Control Application (DCCA) server is down, and the Credit-Control-Fault-Handling (CCFH) action is set to default (terminate), PDP sessions are being converted to postpaid sessions instead of being terminated.

  Workaround: There is currently no known workaround.

- CSCtr22435

  When a new APN with charging characteristics is unconfigured, a traceback occurs.

  This condition occurs when a new access point is configured with charging characteristics, and then the access point is unconfigured.

  Workaround: There is currently no known workaround.

- CSCtr22870

  When PPP PDP type sessions are created, the transmit and receive counters displayed by using the the **show gprs gtp pdp** privileged EXEC command continuously increase even without traffic. The counters are getting incremented due to PPP LCP echo requests and responses.

  This condition occurs only with PPP PDP type subscribers from Cisco IOS Release 12.4(24)YE4 and later.

  Workaround: There is currently no known workaround.

- CSCtr22984

  An SNMP walk for AAA-SERVER-MIB causes delayed **show** and configuration commands and delayed responses to SNMP polls.

  This condition occurs when RADIUS is configured with more than 30 server entries using the following command:

  radius-server host *ip addr* **auth-port 1645 acct-port 1646**

  Workaround: Instead of using the radius-server host command, use the aaa group server radius command to configure the RADIUS servers.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE5:

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 and later single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

  ```
  sup#delete sami#7-fs:core/*.*
  Delete filename [core/*.*]?
  Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
  ```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

  Workaround: There is currently no known workaround.

Miscellaneous Open Caveats

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE5:

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE5. Only severity 1 and 2 caveats and select severity 3 caveats are listed

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

Cisco GGSN Resolved Caveats

This section lists GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(24)YE5.

- CSCto79469

  With the single IP architecture, when a local IP address pool contains just a few IP addresses (for example, less than 10), the block count on the Cisco SAMI Proxy Control Processor (PCOP) increments (viewable using the **show ip local pool** privileged EXEC command) even though there are some addresses available in the pool.

- CSCto83433

  When the Cisco GGSN is running Cisco IOS Release 12.4(24)YE3 or later, frequently clearing the signalling path using the **clear gprs gtp pdp-context path** privileged EXEC command on the Cisco GGSN causes a traceback to occur.

- CSCtq02205 (duplicate of CSCtg91265)

  The **show gprs charging status access-point** *access-point-index* command output displays negative values for the following fields:

  - Number of CDRs
  - Numbers of closed CDRs buffered
  - Number of Containers
  - Number of service records

  This condition occurs when the primary and secondary charging gateway or storage device is unreachable, and more PDP contexts are closed and opened, causing the closed buffered CDRs value to peak to a higher value.

  Workaround: There is currently no known workaround.

- CSCtq36777

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

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

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

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

- CSCtq83301

  High CPU on the Cisco SAMI Traffic and Control Plane processors (TCOPs) in the GTP management process prevent create PDP context requests from being answered.

  This condition occurs with the Cisco GGSN Cisco IOS Release 12.4(24)YE4 image with non-transparent APNs.

- CSCtq83427

  When the Cisco GGSN is configured to allocate the IP addresses to PDP contexts using a RADIUS, and RADIUS allocates a duplicate IP address by mistake, while the PDP is rejected, the GGSN inadvertently sends Accounting Start and Accounting Stop messages for the duplicate users.

  This condition occurs when the GGSN uses a RADIUS IP address allocation and the RADIUS allocates duplicate IP addresses to PDPs.

- CSCtr09022

  The Cisco GGSN experiences SNMP MIB polling time outs, delayed responses to **show** and configuration commands when object identifiers (OIDs) related to AAA-SERVER-MIB are polled.

  This condition occurs when the AAA-SERVER-MIB related OIDs need to polled from the SNMP server, and a large list of AAA server-groups have been configured.

- CSCtr16900

  When a newly configured APN is unconfigured, the GGSN crashes.

  This condition occurs when you configure a new access point and then unconfigure it. This condition does not occur when the **charging profile** access point configuration command is configured under the new APN and then the new APN is unconfigured.

Cisco SAMI Resolved Caveats

This section lists the Cisco SAMI caveats that are resolved with Cisco IOS Release 12.4(24)YE5.

- CSCth24347

  When the Lawful Intercept feature is used, a Safeblk memory leak occurs, which depletes the Safeblk memory.

Caveats - Cisco IOS Release 12.4(24)YE4

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.2, Cisco IOS Release 12.4(24)YE4 image:

- Open Caveats, page 16
- Resolved Caveats, page 19

Open Caveats

Note Caveats that are open in the most current 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 17
- Cisco SAMI Open Caveats, page 19
- 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(24)YE4:

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtn49917

  When the RADIUS Controlled Redirection feature is enabled, when a prepaid subscriber is converted to a postpaid subscriber, the conversion is not synchronized to the standby GGSN. In the standby GGSN, the subscriber continues to be a postpaid user only.

  This condition occurs only when RADIUS Controlled Redirection is enabled when running Cisco IOS Release 12.4(24)YE3.

  Workaround: Disable the RADIUS Controlled Redirection feature.

- CSCto79469

  With the single IP architecture, when a local IP address pool contains just a few IP addresses (for example, less than 10), the block count on the Cisco SAMI Proxy Control Processor (PCOP) increments (viewable using the **show ip local pool** privileged EXEC command) even though there are some addresses available in the pool.

  Workaround: Configure more IP addresses within the local IP address pool range.

- CSCto83433

  When the Cisco GGSN is running Cisco IOS Release 12.4(24)YE3 or later, frequently clearing the signalling path using the **clear gprs gtp pdp-context path** privileged EXEC command on the Cisco GGSN causes a traceback to occur.

  Workaround: There is currently no known workaround.

- CSCto88380

  Even with charging characteristics reject configured (by using the **gprs charging characteristics reject** global configuration command), the GGSN selects the default charging profile for an unmatched charging characteristic value instead of sending a negative response to the SGSN as designed.

  This condition occurs when the GGSN is configured to reject Create PDP Context requests for which no charging profile can be selected.

  Workaround: There is currently no known workaround.

- CSCtq02205

  The **show gprs charging status access-point** *access-point-index* command output displays negative values for the following fields:

  - Number of CDRs
  - Numbers of closed CDRs buffered
  - Number of Containers
  - Number of service records

  This condition occurs when the primary and secondary charging gateway or storage device is unreachable, and more PDP contexts are closed and opened, causing the closed buffered CDRs value to peak to a higher value.

  Workaround: There is currently no known workaround.

- CSCtq15071

  When the Diameter Credit Control Application (DCCA) server is down, and the Credit-Control-Fault-Handling (CCFH) action is set to default (terminate), PDP sessions are being converted to postpaid sessions instead of being terminated.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE4:

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 and later single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

```
sup#delete sami#7-fs:core/*.*
Delete filename [core/*.*]?
Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

  Workaround: There is currently no known workaround.

Miscellaneous Open Caveats

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE4:

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE4. Only severity 1 and 2 caveats and select severity 3 caveats are listed

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

Cisco GGSN Resolved Caveats

This section lists GGSN-specific caveats that are resolved in Cisco IOS Release 12.4(24)YE4.

- CSCtn07756

  In a Cisco GGSN/PGW with a Cisco CSG2 implementation, the quota server interface goes down in few of the Cisco SAMI PowerPCs (PPCs) after a reload occurs.

  This condition occurs only after the Cisco GGSN/PGW is reloaded and the Cisco CSG2 is not.

- CSCto36654

  The Cisco GGSN address allocation fails when a PDP session is being reassigned.

  This condition occurs when a PDP session is being reassigned from one Cisco SAMI Traffic Processor (TCOP) to another. The reason for the reassignment could be that the TCOP does not have a free IP address to allocate to the PDP, so the PDP is reassigned to a TCOP that has a free IP address.

- CSCto43599

  In the Cisco GGSN Cisco IOS 12.4(24)YE3 image, the syntax of the **redirect all ip** command changed to **redirect all**.

  Although the new syntax is accepted, in the running configuration, the command syntax is **redirect all ip**. Therefore, after a reload, the command is rejected.

- CSCto52695

  The number of connections to Traffic and Control Plane processors (TCOPs) shows the maximum connection value when in fact, only a limited number of sessions actually exist.

- CSCto58373

  The following message continuously displays when CPU utilization is over 90 percent.

  ```
  GPRSFLTMG-0-GTPv1NORESOURCE "Number of pending signalling messages reaches limit"
  ```

  This condition occurs on the active GGSN when it receives a changed restart counter from an SGSN post switchover.

- CSCto58589

  RADIUS controlled redirection RCR is not enabled when using a value like "gprs:url-redirect."

  This condition occurs when you configure a domain name as "gprs:url-redirect" in a RADIUS profile. The GGSN is unable to create an RCR-enabled PDP context.

- 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.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

Cisco SAMI Resolved Caveats

This section lists the Cisco SAMI caveats that are resolved with Cisco IOS Release 12.4(24)YE4.

- CSCtn46664

  A duplicate IP is seen in an active SAMI (card 1) when another SAMI (card 2) with the same configuration as card 1 is booting up even though no SVCLC (service line card) is configured for card 2.

  When traffic is sent in card 1 when a duplicate IP is occurring, there might be an impact to traffic.

- 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)
  ```

- CSCto72922

  Packets larger than 3072 bytes, which is the maximum supported packet size for the Cisco SAMI, are being forwarded to the Cisco SAMI PowerPCs (PPCs), causing the following error message to display:

  ```
  %ETSEC-1-ERROR_INT_CAUSE IEVENT_BABR
  ```

  This condition occurs when packets larger than 3072 bytes are forwarded to the Cisco SAMI.

Miscellaneous Resolved Caveat

This section lists an additional miscellaneous caveat that is resolved in Cisco IOS Release 12.4(24)YE4:

- 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.

Caveats - Cisco IOS Release 12.4(24)YE3e

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3e image:

- Open Caveats, page 47
- Resolved Caveats, page 48

Open Caveats

Note Caveats that are open in the most current 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 47
- Cisco SAMI Open Caveats, page 48

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)YE3e.

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtf23298

  High CPU usage occurs.

  This condition occurs when a Terminal Access Controller Access-Control System (TACACS) server is configured with a single connection.

  Workaround: Remove the single connection option.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE3e.

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

  ```
  sup#delete sami#7-fs:core/*.*
  Delete filename [core/*.*]?
  Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
  ```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE3e. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco GGSN Resolved Caveats, page 49
- Cisco SAMI Resolved Caveat, page 50
- Miscellaneous Resolved Caveats, page 50

Cisco GGSN Resolved Caveats

This section lists GGSN caveats that are resolved in Cisco IOS Release 12.4(24)YE3e.

- CSCty60608

  The Cisco GGSN gateway rejects PDP contexts because of the following error:

  ```
  %GPRSFLTMG-0-GTPv1NORESOURCE: GSN: <IP Address>, TEID: <TEID#>, APN: <APN name>,
  MSISDN: <MSISDN>, Reason: 3, System failure
  ```

  This condition occurs when the Network Behind the Mobile feature is configured under an APN as seen in bold in the following example configuration:

  ```
  access-point XXX
     access-point-name YYY
     access-mode non-transparent
     ip-address-pool radius-client
     aggregate X.X.X.0 255.255.255.0
     vrf VRF-NAME
     network-behind-mobile
     redirect all ip <IP>
     dns primary <IP> secondary <IP>
  ```

  Additionally, stale routes under the Traffic and Control Plane processors (TCOPs) display when the **execute-on all show ip route vrf** command is executed.

- CSCty97050

  The IP address pools on the active GGSN and the standby GGSN are not in sync.

  This condition is seen when the **show ip local pool** command is issued on both the standby and active gateway.

  This is a counter issue on the PCOP because with Cisco GGSN Release 10 and later, IP address allocation occurs on the Traffic and Control Plane processors (TCOPs).

- CSCud47003

  The Cisco GGSN crashes while freeing a PDP context.

  This condition occurs when a newly active GGN receives a create on create PDP context request.

- CSCud93452

  The Cisco GGSN crashes when it receives an invalid APN AVP from a RADIUS server.

  This condition occurs when the APN name does not exist in APN list configured on the GGSN or when an APN AVP with an invalid length, etc., is received.

- CSCue57186

  The **show gprs gtp statistics** command and **show gprs access-point statistics all** command do not contain the number of update PDP context requests received.

  This is not a condition and is observed in prior releases of GGSN as well.

  For more information, see the "New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YE3e" section on page 17.

Cisco SAMI Resolved Caveat

There are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)YE3e.

Miscellaneous Resolved Caveats

This section lists the miscellaneous caveats resolved with Cisco IOS Release 12.4(24)YE3e.

- CSCuc54989

  The Cisco SAMI crashes when the **no ip csg iscsi profile** command is issued.

- CSCud87639

  The following error message displays, followed by a traceback:

  ```
  %IFS-3-FSMAX: Failed to add sda4, maximum filesystems 64
  ```

  This condition occurs when an operator configures **ip csg iscsi profile FAS-POZ-A** format and then unconfigures the format using the **no** form of the command.

Caveats - Cisco IOS Release 12.4(24)YE3d

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3d image:

- Open Caveats, page 55
- Resolved Caveats, page 56

Open Caveats

Note Caveats that are open in the most current 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 50
- Cisco SAMI Open Caveats, page 51
- Miscellaneous Open Caveats, page 56

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)YE3d.

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtn49917

  When the RADIUS Controlled Redirection feature is enabled, when a prepaid subscriber is converted to a postpaid subscriber, the conversion is not synchronized to the standby GGSN. In the standby GGSN, the subscriber continues to be a postpaid user only.

  This condition occurs only when RADIUS Controlled Redirection is enabled when running Cisco IOS Release 12.4(24)YE3.

  Workaround: Disable the RADIUS Controlled Redirection feature.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE3d.

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

  ```
  sup#delete sami#7-fs:core/*.*
  Delete filename [core/*.*]?
  Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
  ```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

  Workaround: There is currently no known workaround.

Miscellaneous Open Caveats

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE3d.

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE3d. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

Cisco GGSN Resolved Caveats

This section lists GGSN caveats that are resolved in Cisco IOS Release 12.4(24)YE3d.

- CSCts74384

  For PPP-Regen users, the Time to Live (TTL) value of the IP packet in the downstream direction (from L2TP network server [LNS] to mobile subscriber [MS]), is decremented by 1, whereas in the upstream direction (from MS to LNS server), the TTL value is not decremented.

  This condition occurs only for PPP-Regen users.

- CSCts79810

  Input errors are seen on Cisco GGSN Traffic and Control Plane processors (TCOPs) with specific traffic patterns and signaling.

  This condition occurs when the idle timeout value is configured to a low value (300 seconds). When the idle timeout value is configured to a higher value (for example, 3600 or 7200 seconds), the input errors are not seen.

- CSCtu04654

  The Cisco GGSN Proxy Control Processor (PCOP) might drop RADIUS packets that are encapsulated over GRE tunnel and sent to the GGSN.

  This issue applies to any RADIUS packet that is encapsulated over a GRE tunnel, with or without VPN Routing and Forwarding (VRF).

- CSCtu24158

  The Cisco GGSN might potentially reload at “gprs_ipfib_validate_addrs().”

  This condition is possibly created by a race condition in the application code. Typically, the condition might happen during user handoff (from one SGSN to another) and for that same user upstream user data packets with the wrong MN IP address are received.

- CSCtw63086

  The history displayed by using the **show gprs throughput history** command is not synced with the Proxy Control Processor (PCOP) at the interval configured with the **gprs throughput intervals** command. Therefore, the PCOP does not show the aggregated value for the interval.

- CSCtw79026

  The “InUse” counter is set in the **show ip local pool** command output on the Proxy Control Processor (PCOP) even when there are zero (0) PDP contexts.

  This condition is seen when a burst of PDP deletions occurs or a session flap at 1500 cps.

- CSCtw85850

  The Cisco GGSN does not accept fragmented RADIUS responses (Access-Accept) encapsulated over general encapsulated tunnel (GRE) tunnel. The fragment re-assembly timeout increments during the re-assembly of the packet in the Traffic and Control Plane processor (TCOP) when the first fragment reaches the TCOP, but the trailing fragment goes to the Proxy Control Processor (PCOP) and hence, the Radius response is dropped.

- CSCtv12182

  Data traffic over general encapsulated (GRE) tunnels with packet sizes larger the 1476 bytes are not switched through GGSN.

  This condition occurs when the GRE tunnel endpoint on the Gi (PDN side) is configured with a value greater than 1476 bytes, which leads to the fragmentation of IP/GRE when a data packet is larger than 1476 bytes.

Cisco SAMI Resolved Caveat

There are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)YE3d.

Miscellaneous Resolved Caveats

This section lists the miscellaneous caveats that are resolved with Cisco IOS Release 12.4(24)YE3d.

- CSCsk03336

  Interface counters on line cards might show incorrect packet input statistics in the **show interface** command output.

  This condition occurs when the “CEF LC IPC Backg” process causes the line card CPU to exceed 90%. This is seen when an unstable network causes excessive Cisco Express Forwarding (CEF) updates.

- CSCte89022

  Gateway might reload while handling a Virtual Private Dialup Network (VPDN) call due to invalid memory reference.

- CSCti46171

  Cisco IOS Software contains four vulnerabilities related to Cisco IOS Zone-Based Firewall features. These vulnerabilities are as follows:

  - Memory Leak Associated with Crafted IP Packets
  - Memory Leak in HTTP Inspection
  - Memory Leak in H.323 Inspection
  - Memory Leak in SIP Inspection

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-zbfw

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow 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. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

- CSCtr49064

  The Secure Shell (SSH) server implementation in Cisco IOS Software and Cisco IOS XE Software contains a denial of service (DoS) vulnerability in the SSH version 2 (SSHv2) feature. An unauthenticated, remote attacker could exploit this vulnerability by attempting a reverse SSH login with a crafted username. Successful exploitation of this vulnerability could allow an attacker to create a DoS condition by causing the device to reload. Repeated exploits could create a sustained DoS condition.

  The SSH server in Cisco IOS Software and Cisco IOS XE Software is an optional service, but its use is highly recommended as a security best practice for the management of Cisco IOS devices. Devices that are not configured to accept SSHv2 connections are not affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCts38429

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

Caveats - Cisco IOS Release 12.4(24)YE3c

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3c image:

Open Caveats

Note Caveats that are open in the most current 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

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)YE3c.

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtn49917

  When the RADIUS Controlled Redirection feature is enabled, when a prepaid subscriber is converted to a postpaid subscriber, the conversion is not synchronized to the standby GGSN. In the standby GGSN, the subscriber continues to be a postpaid user only.

  This condition occurs only when RADIUS Controlled Redirection is enabled when running Cisco IOS Release 12.4(24)YE3.

  Workaround: Disable the RADIUS Controlled Redirection feature.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE3c.

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

  ```
  sup#delete sami#7-fs:core/*.*
  Delete filename [core/*.*]?
  Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
  ```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

  Workaround: There is currently no known workaround.

Miscellaneous Open Caveats

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE3c.

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE3c. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco GGSN Resolved Caveats, page 57
- Cisco SAMI Resolved Caveat, page 57
- Miscellaneous Resolved Caveat, page 58

Cisco GGSN Resolved Caveats

This section lists GGSN caveats that are resolved in Cisco IOS Release 12.4(24)YE3c.

- CSCts78280

  In an enhanced GGSN (eGGSN) implementation, which is the Cisco GGSN and Cisco CSG2 configured together to provide enhanced service-aware billing, the eGGSN is unable to establish PDPs for service-aware postpaid subscribers.

  This condition occurs only with a service-aware postpaid eGGSN configuration with the Cisco IOS Release 12.4(24)YE3b image.

- CSCts84654

  The Cisco GGSN drops a create PDP context request when the source IP address of the create PDP context request is different from the GPRS support node (GSN) IP address in the GTP header.

  This condition occurs only with Cisco IOS Release 12.4(24)YE3a and later when the source IP address of the create PDP context request is different from the GSN IP address.

- CSCtt07560

  In a redundant implementation, the following traceback appears on the active GGSN for a brief period of time during the bootup.

  ```
  %IDMGR-3-INVALID_ID: bad id in id_delete (id: 0xD0D0D0C),
  ```

  This condition occurs only in a redundant implementation when the redundancy state of a GGSN is not yet “ACTIVE.” Once the GGSN state is “ACTIVE,” the traceback stops displaying.

Cisco SAMI Resolved Caveat

This section lists a Cisco SAMI caveat that is resolved with Cisco IOS Release 12.4(24)YE3c.

- CSCsx82030

  A specific configuration sequence causes a configuration download/parse error on the SAMI.

  The condition is logged as follows:

  ```
  SAMI 1/3: Feb 18 09:27:43.779: %IPC-0-CFG_DOWNLOAD_ERROR: Configuration
  download/parse error: Failed to download config on one or more processors,
  traffic will get blocked -Process= "Init", ipl= 0, pid= 3
  ```

  If inter-device redundancy is configured, a peer SAMI might reload with the redundancy framework (RF)/Cisco IOS Hot Standby Routing Protocol (HSRP) state broken.

  The following configuration sequence causes the configuration download/parse error:

  a. The “snmp-server community” is using a standard ACL.
  b. The standard ACL is removed.
  c. A new extended ACL is created with the same name as the previous standard ACL.
  d. The SAMI is reloaded.

  After the reload, the SAMI receives the configuration download/parse error.

Miscellaneous Resolved Caveat

This section lists a miscellaneous resolved caveat that is resolved with Cisco IOS Release Cisco IOS Release 12.4(24)YE3c.

- CSCtb39102

  In a redundant implementation, a session is not synchronized to a standby unit if the MTU of the Gigabit0/0 interface of the active SAMI is set to1600 bytes. The router could also perform a redundancy framework (RF) self-reload.

Caveats - Cisco IOS Release 12.4(24)YE3b

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3b image:

- Open Caveats, page 58
- Resolved Caveats, page 60

Open Caveats

Note Caveats that are open in the most current 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 58
- Cisco SAMI Open Caveats, page 59
- Miscellaneous Open Caveats, page 59

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)YE3b.

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtn49917

  When the RADIUS Controlled Redirection feature is enabled, when a prepaid subscriber is converted to a postpaid subscriber, the conversion is not synchronized to the standby GGSN. In the standby GGSN, the subscriber continues to be a postpaid user only.

  This condition occurs only when RADIUS Controlled Redirection is enabled when running Cisco IOS Release 12.4(24)YE3.

  Workaround: Disable the RADIUS Controlled Redirection feature.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE3b.

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

```
sup#delete sami#7-fs:core/*.*
Delete filename [core/*.*]?
Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

  Workaround: There is currently no known workaround.

Miscellaneous Open Caveats

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE3b.

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE3b. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

Cisco GGSN Resolved Caveats

This section lists GGSN caveats that are resolved in Cisco IOS Release 12.4(24)YE3b.

- CSCso02147

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCth03022

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

- CSCth11006

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCti48504

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

- CSCti48483

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCtj04672

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

- CSCtq15071

  When the Diameter Credit Control Application (DCCA) server is down, and the Credit-Control-Fault-Handling (CCFH) action is set to default (terminate), PDP sessions are being converted to postpaid sessions instead of being terminated.

- CSCtq36777

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

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

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

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

- CSCtq83301

  High CPU on the Cisco SAMI Traffic and Control Plane processors (TCOPs) in the GTP management process prevent create PDP context requests from being answered.

  This condition occurs with non-transparent APNs.

- CSCtr09665

  When a non existent or failed Diameter server is configured on the Cisco GGSN, it might exhaust all available sockets for Diameter communication.

- CSCtr20156

  A high CPU in the GTP management process occurs, with "No Resource Pending" signal messages.

  This condition occurs when RADIUS cannot be reached or the connection is flapping. The PDPs that are waiting for a RADIUS response are marked for deletion.

- 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.

- CSCtr30916

  A GTPv0 create request over an existing GTPv1 PDP causes a high CPU.

  This condition occurs only when the existing GTPv1 PDP is waiting for the completion of an update request and then a GTPv0 create is initiated.

  (CSCtr31369 and CSCtr30916 fix the symptom and free the CPU by dropping the new GTPv0 create request.)

- CSCtr31369

  A GTPv0 create request over an existing GTPv1 PDP causes a high CPU.

  This condition occurs only when the existing GTPv1 PDP is waiting for the completion of an update request and then a GTPv0 create is initiated.

  (CSCtr31369 and CSCtr30916 fix the symptom and free the CPU by dropping the new GTPv0 create request.)

- CSCtr42950 (Duplicate of CSCtr56632)

  The Cisco GGSN might arrive in a situation in which the CPU on certain Traffic and Control Plane processors (TCOPs) reaches almost 100%. When this condition occurs, stuck PDP sessions are also seen on the affected TCOPs.

  This condition causes subscribers to experience problems in the GTP control path (for example, setting up PDP sessions) and in the data path (for example, sending data through the PDP session). This condition typically occurs in a service-aware implementation and appears to begin when the GGSN assumes a path restart has occurred, which indicates that the SGSN is restarting, when in fact, that is not the case.

- 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.

- CSCtr56632

  When path deletion is triggered by a new recovery information element (IE) value, the GGSN does not support the creation of new PDPs until the path is completely deleted.

  This condition worsens when there is a stuck PDP in the path being deleted, the GGSN does not allow the creation of any PDPs until the old path is deleted, and the path cannot be deleted because of the stuck PDP. This situation is called a “deadlock.”

- CSCtr61654

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

- CSCtr61828

  The Cisco GGSN always sends the default Dynamic Feedback Protocol (DFP) weight of 8 to the Cisco IOS SLB on the supervisor regardless of the weight dynamically reported by the individual Traffic and Control Plane processors (TCOPs).

- CSCtr66659

  The Cisco GGSN load balancer state becomes stuck in a DFP_THROTTLED state when the maximum number of PDPs are created, and it is unable to exit from this state when the number of PDPs decreases. This condition occurs when GGSN is reporting dynamic weights to a Dynamic Feedback Protocol (DFP) manager like GTP SLB.

- CSCtr87690

  The GGSN does not create PDPs even when there is sufficient IP address space. The RefCount in the International Mobile Subscriber Identity (IMSI) sticky database is negative one (-1).

```
GGSN#show sami sm imsi
IMSI: 214350000000001, Permanent: NO,  Location: 7
  MSISDN: 91214365060000000F100  Length:9
  RefCount:-1, version:1, SeqNum:2, NSAPI_MAP:0000
IMSI: 214350000000002, Permanent: NO,  Location: 4
  MSISDN: 9121436506000000F200  Length:9
  RefCount:-1, version:1, SeqNum:2, NSAPI_MAP:0000
```

  This condition occurs with a single IP architecture (Proxy Control Processor [PCOP] and Traffic and Control Plane processors [TCOP]) when all the IP addresses in a TCOP are “In Use” and the TCOP attempts a reassignment. The PCOP fails to reassign the session because of the RefCount -1.

- CSCtr90757

  The GGSN retransmits a lot of RADIUS Accounting Start requests for postpaid subscribers. The current behavior is as follows:

  a. The GGSN sends a RADIUS Accounting Start.
  b. The Cisco Content Services Gateway-2nd Generation (CSG2) sends a Gx Diameter Credit Control Request (CCR-I) to the Policy Control and Charging Rules Function (PCRF).
  c. The PCRF sends a Credit Control Answer (CCA-I) with either a 4001 or 5003 result code.
  d. The CSG2 sends a RADIUS Change of Operation (CoA) with AUTH_FAILED (0x02).
  e. The GGSN acknowledges the CoA but retransmits the Accounting Start, causing a lot of retransmission until the RADIUS times out.

  In this scenario, the GGSN relies on the RADIUS timeout and the signaling impacts the network.

  The desired behavior is for the GGSN to not retransmit the RADIUS Accounting Start request after receiving a CoA with Auth_failed but instead send a Create PDP Context Deny.

  This condition occurs with postpaid subscribers, whom are not allowed to use the Gx PCRF.

- CSCtr93403

  The following syslog message appears intermittently on the GGSN:

```
GPRSFLTMG-4-CHARGING: GSN: 0.0.0.0, TID: 0000000000000000, APN: NULL, Reason: 13,
Trying to close a NULL cdr_entry
```

  This condition occurs even when the charging function is not configured.

- CSCts05678

  There is a mismatch of the local IP address pool “In Use” count between the Proxy Control Processor (PCOP) and Traffic and Control Plane processors (TCOP). This occurs because some of the IP address in the PCOP are not freed even though the PDP context is cleared.

  For example:

```
GGSN#show gprs gtp status
GPRS GTP Status:
  activated gtpv0 pdp     0
  activated gtpv1 pdp     0
  activated ms            0
  activated ipv6 ms       0
  activated gtpv0 v6 pdp  0
  activated gtpv1 v6 pdp  0
  activated ppp regen pdp 0
  activated ppp pdp       0
```

```
  gtp's va hwidbs         0
  gtp's va swidbs         0
  gtp ipv6 swidbs         0
  gtp direct tunnel PDPs  0
Service-aware Status:
  Prepaid PDPs            0
  Postpaid PDPs           0
IST-GGSN-07#sh ip lo
IST-GGSN-07#sh ip local poo
IST-GGSN-07#sh ip local pool

Pool                    Begin           End             Free  In use   Blocked
** pool <internet> is in group <internet>
internet                178.241.128.0   178.241.255.255 32744      24       0
                         188.57.192.0    188.57.255.255  16373      11       0
                         188.58.96.1     188.58.127.255  8184       7        0
                         31.142.96.0     31.142.127.255  8188       4        0
** pool <wap> is in group <wap>
wap                     10.51.0.1       10.51.254.255   64798     481       0
** pool <mgb> is in group <mgb>
mgb                     188.59.176.1    188.59.191.255  4095       0        0
** pool <streaming> is in group <streaming>
streaming               10.52.80.1      10.52.87.255    2044       3        0
** pool <test15> is in group <test15>
test15                  31.142.96.0     31.142.127.255  8192       0        0
```

- CSCts12533

  While PDPs are being created, the following traceback might display:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_delete (id: 0xD0D0D0C),  -Traceback= 0x460E1CC4z
  0x442FA37Cz 0x442DFB94z 0x442D2A28z 0x442D35ECz 0x45943804z 0x45946EE4z
  ```

  This traceback might could display during a rare condition in which several hundred PDPs are opened at high rate.

- CSCts23411

  Sometimes, the tunnel identifier (TID) value in a GTPv0 create PDP context response is corrupt.

  This condition occurs with roaming subscribers.

Cisco SAMI Resolved Caveat

This section lists a Cisco SAMI caveat that is resolved with Cisco IOS Release 12.4(24)YE3b.

- CSCtc95114

  When performing a write memory or copying a file to the bootflash of a PowerPC (PPC), the Cisco SAMI drops a few packets.

Miscellaneous Resolved Caveat

This section lists a miscellaneous resolved caveat that is resolved with Cisco IOS Release Cisco IOS Release 12.4(24)YE3b.

- CSCtl48268

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

Caveats - Cisco IOS Release 12.4(24)YE3a

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3a image:

Open Caveats

Note Caveats that are open in the most current 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

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)YE3a.

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtn49917

  When the RADIUS Controlled Redirection feature is enabled, when a prepaid subscriber is converted to a postpaid subscriber, the conversion is not synchronized to the standby GGSN. In the standby GGSN, the subscriber continues to be a postpaid user only.

  This condition occurs only when RADIUS Controlled Redirection is enabled when running Cisco IOS Release 12.4(24)YE3.

  Workaround: Disable the RADIUS Controlled Redirection feature.

- CSCtq15071

  When the Diameter Credit Control Application (DCCA) server is down, and the Credit-Control-Fault-Handling (CCFH) action is set to default (terminate), PDP sessions are being converted to postpaid sessions instead of being terminated.

  Workaround: There is currently no known workaround.

- 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.

  Workaround: There is no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE3a.

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

```
sup#delete sami#7-fs:core/*.*
Delete filename [core/*.*]?
Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

  Workaround: There is currently no known workaround.

Miscellaneous Open Caveats

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE3a.

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE3a. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco GGSN Resolved Caveats, page 69
- Cisco SAMI Resolved Caveats, page 71
- Miscellaneous Resolved Caveats, page 72

Cisco GGSN Resolved Caveats

This section lists GGSN caveats that are resolved in Cisco IOS Release 12.4(24)YE3a.

- CSCte97852

  Some of the Cisco SAMI Traffic and Control Plane processors (TCOPs) are move to a MAXCONNS state and the number of connections reach the maximum value even though the actual number of sessions in a TCOPs are few as is displayed by the **show ip slb real** command:

```
sami-7#show ip slb real

real                  server farm      weight  state          conns
-------------------------------------------------------------------
127.0.0.94            CISCO-LB-SFAR    3       OPERATIONAL    0
127.0.0.95            CISCO-LB-SFAR    3       MAXCONNS       4294967295
127.0.0.96            CISCO-LB-SFAR    3       MAXCONNS       0
127.0.0.97            CISCO-LB-SFAR    3       MAXCONNS       0
127.0.0.98            CISCO-LB-SFAR    3       MAXCONNS       0
sami-7#
```

  This condition occurs with the Single IP architecture.

- CSCtq02205 (duplicate of CSCtg91265)

  The **show gprs charging status access-point** *access-point-index* command output displays negative values for the following fields:

  - Number of CDRs
  - Numbers of closed CDRs buffered
  - Number of Containers
  - Number of service records

  This condition occurs when the primary and secondary charging gateway or storage device is unreachable, and more PDP contexts are closed and opened, causing the closed buffered CDRs value to peak to a higher value.

- CSCtg91265

  An R99 charging status mismatch with the status under the APN occurs. The discrepancy is viewable by using the **show gprs charging status** command and the **show gprs charging status** access-point command.

  This condition occurs when one session with multiple CDRs exists.

- CSCtj98858

  When handoffs from GTPv1 to GTPv0 occur for a large number of PDP contexts, and then all of the GTPv0 PDP contexts are deleted, an unexpected error “real->num_conns-with real = 0 in rr_real_conn_remove” and tracebacks occur.

- CSCtn07756

  In a Cisco GGSN/PGW with a Cisco CSG2 implementation, the quota server interface goes down in few of the Cisco SAMI PowerPCs (PPCs) after a reload occurs.

  This condition occurs only after the Cisco GGSN/PGW is reloaded and the Cisco CSG2 is not.

- CSCto36654

  The Cisco GGSN address allocation fails when a PDP session is being reassigned.

  This condition occurs when a PDP session is being reassigned from one Cisco SAMI Traffic and Control Plane Processor (TCOP) to another. The reason for the reassignment could be that the TCOP does not have a free IP address to allocate to the PDP, so the PDP is reassigned to a TCOP that has a free IP address.

- CSCto43599

  In the Cisco GGSN Cisco IOS 12.4(24)YE3 image, the syntax of the **redirect all ip** command changed to **redirect all**.

  Although the new syntax is accepted, in the running configuration, the command syntax is **redirect all ip**. Therefore, after a reload, the command is rejected.

- CSCto52695

  The number of connections to TCOPs shows the maximum connection value when in fact, only a limited number of sessions actually exist.

- CSCto58373

  The following message continuously displays when CPU utilization is over 90 percent.

  GPRSFLTMG-0-GTPv1NORESOURCE "Number of pending signalling messages reaches limit"

  This condition occurs on the active GGSN when it receives a changed restart counter from an SGSN post switchover

- CSCto58589

  RADIUS controlled redirection RCR is not enabled when using a value like "gprs:url-redirect."

  This condition occurs when you configure a domain name as "gprs:url-redirect" in a RADIUS profile. The GGSN is unable to create an RCR-enabled PDP context.

- 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.

- CSCto75983

  When the Cisco GGSN receives a changed recovery information element (IE), it restarts the path, thereby deleting the existing PDP contexts on the path and creating new PDP contexts for requests that have arrived with an updated recovery IE.

  When this delete and create message information is synchronized to the standby GGSN, the Proxy Control Processor (PCOP) of the standby GGSN might send a negative response for an International Mobile Subscriber Identity (IMSI) create message from a Traffic and Control Plane processor (TCOP), especially when the path that is restarting has higher number of sessions (60k+).

  The negative response sent by the PCOP enables the TCOP on standby to retry the IMSI create. In the retry path, a startover start of timer is performed instead of restart start. This causes the serv timer links to become corrupt, which leads to the standby GGSN crashing.

- CSCto79469

  With the single IP architecture, when a local IP address pool contains just a few IP addresses (for example, less than 10), the block count on the Cisco SAMI Proxy Control Processor (PCOP) increments (viewable using the **show ip local pool** privileged EXEC command) even though there are some addresses available in the pool.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

Cisco SAMI Resolved Caveats

This section lists the Cisco SAMI caveat that is resolved with Cisco IOS Release 12.4(24)YE3a.

- CSCtc60025

  When one of the Cisco SAMI daughter cards has a sudden hardware failure during run time, such as a reset circuitry failure, the control processor fails to detect the failure and assumes that the system is UP. The supervisor engine continues to display the Cisco SAMI status as OK. The standby unit remains unaware of the active failure, and fails to switch over until the keepalive timeout occurs. This condition results in total outage for minutes until the standby takes over. Under these conditions, the hardware and software watchdogs also fail to act.

- CSCth24347

  When the Lawful Intercept feature is used, a Safeblk memory leak occurs, which depletes the Safeblk memory.

- CSCtn46664

  A duplicate IP is seen in an active SAMI (card 1) when another SAMI (card 2) with the same configuration as card 1 is booting up even though no SVCLC (service line card) is configured for card 2.

  When traffic is sent in card 1 when a duplicate IP is occurring, there might be an impact to traffic.

- 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)

- CSCto72922

  Packets larger than 3072 bytes, which is the maximum supported packet size for the Cisco SAMI, are being forwarded to the Cisco SAMI PowerPCs (PPCs), causing the following error message to display:

  %ETSEC-1-ERROR_INT_CAUSE IEVENT_BABR

  This condition occurs when packets larger than 3072 bytes are forwarded to the Cisco SAMI.

Miscellaneous Resolved Caveats

This section lists the miscellaneous resolved caveat that is resolved with Cisco IOS Release Cisco IOS Release 12.4(24)YE3a.

- 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.

Caveats - Cisco IOS Release 12.4(24)YE3

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.1, Cisco IOS Release 12.4(24)YE3 image:

- Open Caveats, page 26
- Resolved Caveats, page 27

Open Caveats

Note Caveats that are open in the most current 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 22
- Cisco SAMI Open Caveats, page 23
- Miscellaneous Open Caveats, page 24

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)YE3:

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  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.

- CSCtn49917

  When the RADIUS Controlled Redirection feature is enabled, when a prepaid subscriber is converted to a postpaid subscriber, the conversion is not synchronized to the standby GGSN. In the standby GGSN, the subscriber continues to be a postpaid user only.

  This condition occurs only when RADIUS Controlled Redirection is enabled when running Cisco IOS Release 12.4(24)YE3.

  Workaround: Disable the RADIUS Controlled Redirection feature.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YE3:

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available as follows:

```
sup#delete sami#7-fs:core/*.*
Delete filename [core/*.*]?
Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
```

- CSCtk65554

  During a redundancy switchover initiated from a command line interface by using the **redundancy switch-activity force** command, debug information is written in all of the Cisco SAMI processors and collected in the LCP core: like with an RF-induced reload.

  Workaround: There is currently no known workaround.

- CSCtn46664

  A duplicate IP is seen in an active SAMI (card 1) when another SAMI (card 2) with the same configuration as card 1 is booting up even though no SVCLC (service line card) is configured for card 2.

  When traffic is sent in card 1 when a duplicate IP is occurring, there might be an impact to traffic.

  Workaround: There is currently no known workaround. Do not bring up a SAMI with the same configuration as an existing SAMI while that card is up and active.

Miscellaneous Open Caveats

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE3:

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE3. Only severity 1 and 2 caveats and select severity 3 caveats are listed

- Cisco GGSN Resolved Caveats, page 24
- Cisco SAMI Resolved Caveats, page 25

Cisco GGSN Resolved Caveats

This section lists GGSN caveats that are resolved in Cisco IOS Release 12.4(24)YE3.

- CSCsy77867

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

- 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.

- CSCtk54730

  GTPv0 PDPs are hanging. This condition occurs when the Cisco GGSN is running Cisco IOS Software Release 12.4(22)YE4 and later and is specific to GTPv0 when an SGSN sends a create request for an already existing PDP associated with a virtual APN.

- CSCtk67496

  When adding an application configuration on a Cisco SAMI, the following error message occurs:

  %IPC-4-CFG_SYNC_ERROR: Configuration Sync error: rollback failed, cmd = no exit-address-family -Process= "config rollback", ipl= 0, pid= 172

- CSCtd26768

  When a subscriber attempts to configure a multiline banner message, the session or console prompt goes into an “unknown mode” state and cannot recover.

  This condition is not seen with preexisting multiline banner messages, but only when one is configured at the prompt.

- CSCtl23238

  When a subscriber 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 subscriber 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.

- CSCtl90606

  A traffic leak occurs between the Cisco SAMI and the supervisor engine module even if the **svclc** commands have been removed.

  This condition occurs when an operator installs a new Cisco SAMI, removes the **svclc** module command from the existing Cisco SAMI, and configures the new module exactly like the old one.

- CSCtk76072

  The Cisco GGSN running Cisco IOS Software Release 12.4(24)YE1 and later reloads, and the PC of the reload points to serv_tmr_service_chain routine.

  This condition occurs under rare circumstances while the Cisco GGSN is experiencing high traffic conditions.

- CSCtn14284

  An AAA access-request returns with an internal error, and on the Cisco GGSN the following unconditional bug information is printed: “AAA had an unexpected return.”

  This condition occurs when an access-request is sent to the AAA server during periods of stress conditions on the client process and a failure to build the RADIUS packet occurs.

- 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-number* [*interface-priority*] command is not configured.

- CSCth77234

  The weight of Diameter Credit Control Application (DCCA) profile under the charging profile can't be configured through SNMP. By default, the weight is 1.

  This condition exists when the DCCA profile is configured under a charging profile using SNMP.

- CSCtj35993

  With Cisco GGSN Release 10.0, when the Diameter peer goes down, an SNMP trap appears to not be sent.

- CSCtk04216

  A PDP is not created with a duplicate create PDP context request for local pools.

  This condition occurs when the duplicate PDP is created with the recycle delay configured and there are no addresses present in the Traffic and Control Plane processors (TCOP) to serve the request.

- CSCtn42411

  The downstream traffic volume in GGSN CDRs stays at 0. This condition occurs when an MS has sent or received more than 4 GB of data.

Cisco SAMI Resolved Caveats

This section lists the Cisco SAMI caveat that is resolved with Cisco IOS Release 12.4(24)YE3.

- CSCtj96992

  The iSCSI classified name does not conform to the iSCSI specification. It contains invalid characters.

Caveats - Cisco IOS Release 12.4(24)YE2

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE2 image:

- Open Caveats, page 26
- Resolved Caveats, page 27
- Unreproducible and Closed Caveats, page 31

Open Caveats

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

- Cisco GGSN Open Caveats, page 26
- Cisco SAMI Open Caveat, page 27
- Miscellaneous Open Caveat, page 27

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)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** commands.

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with Cisco Express Forwarding (CEF) enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  Workaround: There is currently no known workaround.

- 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-number* [*interface-priority*] command is not configured.

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

- CSCth77234

  The weight of Diameter Credit Control Application (DCCA) profile under the charging profile cannot be configured through SNMP. By default, the weight is 1.

  This condition exists when the DCCA profile is configured under a charging profile using SNMP.

- CSCtj35993

  With Cisco GGSN Release 10.0, when the Diameter peer goes down, an SNMP trap appears to not be sent.

  Workaround: There is currently no known workaround.

- CSCtk04216

  A PDP is not created with a duplicate create PDP context request for local pools.

  This condition occurs when the duplicate PDP is created with the recycle delay configured and there are no addresses present in the Traffic and Control Plane processors (TCOP) to serve the request.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveat

This section lists the Cisco SAMI caveat that is open with Cisco IOS Release 12.4(24)YE2:

- CSCtj14825

  The Cisco SAMI running the Cisco GGSN Release 10.0 single IP image generates 0 byte crashinfo files on the core: of the Line Control Processor (LCP) when there is no space available on the core.

  This condition occurs only when there is not enough space in the core:

  Workaround: Delete the core: files and ensure enough space is available.

```
sup#delete sami#7-fs:core/*.*
Delete filename [core/*.*]?
Delete sami#7-fs:core/crashinfo_collection-20100923-175329.tar? [confirm]
```

Miscellaneous Open Caveat

This section lists an additional miscellaneous caveat that is open in Cisco IOS Release 12.4(24)YE2:

- CSCtg44918

  The Internet Small Computer System Interface (iSCSI) connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is at approximately 70%, and 50k PDPs exist with downstream traffic flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE2. Only severity 1 and 2 caveats and select severity 3 caveats are listed

- GGSN Resolved Caveats, page 28
- Cisco SAMI Resolved Caveats, page 29
- Miscellaneous Resolved Caveats, page 30

GGSN Resolved Caveats

This section lists GGSN caveats that are resolved in Cisco IOS Release 12.4(24)YE2.

- CSCtb09757

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

- 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**).

- CSCtj20610

  The Cisco GGSN prints the following bug information when there is no debug enabled:

  ```
  gtp_udp_unreachable: path found <mem address>
  ```

  This condition occurs when the GGSN receives an ICMP UNREACHABLE message for the GTP path destination. It prints the above debug even without any debug enabled.

  This debug information is rarely displayed because the ICMP UNREACHABLE is a rare scenario for an existing path.

- CSCtj24869

  The Cisco GGSN R10 single ip image displays the following message:

  ```
  DUP_IPv4ADDR_IN_IXP_PDPACTIVATIONFAIL
  ```

  This condition exists when the following events occur:

  - IPv4 address allocating is being performed by RADIUS
  - RADIUS reallocates the IP address to a different PDP after the IP address has been freed by a closed PDP.
  - The standby GGSN becomes the active GGSN.

- CSCti93144

  When an access control list (ACL) with Layer 4 (L4) information is configured to permit packets with specific L4 information (for example, port range, etc.), the non-initial fragments are dropped. This behavior is dependent on the complete ACL lines. Equivalent undesired behavior might be observed when the ACL is for deny.

  This condition occurs with an ACL with L4 information configured under an APN, and incoming packets (upstream or downstream) have IP fragmentation. With upstream packets, this problem occurs when the inner packets are fragments and the out (GTP) packets are complete.

- CSCtj52610

  The synchronization of PDPs on the GGSN fails, which leads to a high CPU.

- CSCtg18419

  The standby GGSN has less PDP contexts than the active GGSN.

  This condition occurs when IP addresses are assigned from a local pool, and the total number of allocated addresses exceeds 5/6th of the total number of addresses available.

- CSCti61882

  A buffer leak occurs due to an error indication in the Cisco GGSN.

- 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.

Cisco SAMI Resolved Caveats

This section lists Cisco SAMI caveats that are resolved with Cisco IOS Release 12.4(24)YE2.

- CSCti92634

  The Cisco SAMI reloads with an “HM failure” or “RF induced reload” error message.

  This condition occurs when fragmented packets are received by the Cisco SAMI running a Cisco IOS Release 12.4(24)YE1 image.

- CSCtj29848

  The Cisco SAMI LCP crashes and reloads while attempting to collect core dump information. This condition occurs only when the IXP network processor is hung.

- CSCti61842

  The Cisco SAMI reloads with an HM failure.

- CSCtj29100

  The Cisco SAMI crashes when fragmented packets, which do not belong to a valid session, hit a condition that causes the fragments to be dropped.

- CSCej50237

  The Cisco SAMI reloads with an “RF induced reload” error message with a traceback.

  This condition occurs when a momentary communication breakdown between two redundantly configured Cisco SAMIs, leading the SAMIs to active, and causing a reload of one the Cisco SAMIs.

- CSCth66260

  A core file is not written when the following configuration exists, and a PPC crashes:

  ```
  exception core-file abhv/core_4gb compress timestamp
  exception dump 10.153.144.25
  ```

  The following logs are seen:

  ```
  writing crashinfo to bootflash:crashinfo_proc3_20100702-105423
  writing compressed tftp://10.153.144.25/abhv/core_4gb_proc3_20100702-105423.Z
  SAMI 2/3: Jul  2 10:54:23.027: %SYS-2-EXCEPTIONDUMP: System Crashed, Writing
  Core..... [Failed]
  writing compressed tftp://10.153.144.25/abhv/core_4gbiomem_proc3_20100702-105423.Z
  %Error opening tftp://10.153.144.25/abhv/core_4gb_proc3_20100702-105423.Z (Timed
  out)..... [Failed]
  %Error opening tftp://10.153.144.25/abhv/core_4gbiomem_proc3_20100702-105423.Z (Timed
  out)
  ```

  A general **write core** command issued from the command line interface is successful.

- 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.

- CSCtk12410

  When two Cisco SAMIs are configured as an active standby pairs running Cisco IOS Release 12.4(24)YE1, any unexpected reload of one of the processors in the standby SAMI can cause the active SAMI to reload because of an RF induced self-reload.

  This condition occurs if the HSRP priority of the standby SAMI is greater than the priority of the active SAMI, either because of explicit configuration or based on the IP address of the active and standby SAMIs.

Miscellaneous Resolved Caveats

This section lists miscellaneous caveats that are resolved in Cisco IOS Release 12.4(24)YE2.

- CSCsy55362

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

- CSCtj66858

  When using the Cisco RSP720, the **show module** command output shows the software version as the firmware version for the Cisco SAMI.

  This condition occurs when the RSP720 is a part of a redundant implementation and a switchover is forced.

- CSCta49840

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

Unreproducible and Closed Caveats

This section lists caveats that have been closed or not reproduced in Cisco IOS Release 12.4(24)YE2.

- CSCte97577

  The Cisco SAMI resets after the PPCs display an IXP network processor health monitoring failure. This failure message is also present in the collected crash information. On very rare occasions, this issue might occur when thousands of sessions are initiated per second by network behind mobile subscriber (NBMS) users.

Caveats - Cisco IOS Release 12.4(24)YE1

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE1 image:

- Open Caveats, page 31
- Resolved Caveats, page 33
- Unreproducible and Closed Caveats, page 37

Open Caveats

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

- Cisco GGSN Open Caveats, page 31
- Cisco SAMI Open Caveats, page 32
- Miscellaneous Open Caveat, page 33

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)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** commands.

- CSCta98133

  The Cisco GGSN drops the downstream traffic sent over IPv6 PDP with CEF enabled.

  This condition occurs only with downstream traffic. Upstream traffic is switched correctly.

  Workaround: There is currently no known workaround.

- CSCte97577

  The Cisco SAMI resets after the PPCs display an IXP network processor health monitoring failure. This failure message is also present in the collected crash information. On very rare occasions, this issue might occur when thousands of sessions are initiated per second by network behind mobile subscriber (NBMS) users.

  Workaround: There is currently no known workaround.

- CSCtg44918

  The iSCSI connection to the iSCSI target is timed out and terminated when the CPU usage is high, and the disk is not in a usable state even after the TCP connection is re-established.

  This condition occurs when the CPU usage is approximately 70%, and 50k PDPs and downstream traffic is flowing through all the PDPs on the Cisco GGSN.

  This issue occurs with EMC and Linux iSCSI targets.

  Workaround: Unconfigure the **gprs iscsi** command and then reconfigure the command.

- 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-number* [*interface-priority*] command is not configured.

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

- CSCth39785

  When the Cisco GGSN receives a Delete PDP Context request from SGSN and tears down its Layer 2 Tunneling Protocol (L2TP) tunnel to the LNS, the L2TP Call-Disconnect-Notify (CDN) packet sent from the GGSN contains the following Result-Error Code AVP:

```
Result-Error Code AVP
        Result code: 2 - Session disconnected for the reason indicated in Error Code
        Error code: 6 - A generic vendor-specific error occurred
        Error Message: admin-reset/VPDN Admin Disconnect   <<<<<
The Error Message should be "user-requst" instead of "admin-reset".
```

  Workaround: There is currently no known workaround.

- CSCth77234

  The weight of Diameter Credit Control Application (DCCA) profile under the charging profile can't be configured through SNMP. By default, the weight is 1.

  This condition exists when the DCCA profile is configured under a charging profile using SNMP.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

There are no known caveats open in Cisco IOS Release 12.4(24)YE1.

Miscellaneous Open Caveat

This section lists the Miscellaneous caveat that is open in Cisco IOS Release 12.4(24)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, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE1. Only severity 1 and 2 caveats and select severity 3 caveats are listed

- GGSN Resolved Caveats, page 33
- Cisco SAMI Resolved Caveat, page 36
- Other Resolved Caveats, page 36

GGSN Resolved Caveats

This section lists GGSN caveats that are resolved in Cisco IOS Release 12.4(24)YE1.

- CSCte51938

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

- CSCte56779

  A traceback is seen when the quota server interface is unconfigured. This condition occurs only when the enhance quota server interface is not enabled between the Cisco GGSN and Cisco CSG2.

- 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 will have the decoding error.

- 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.

- CSCtf04073

  PDP contexts might become stale when the Cisco GGSN receives more than one change during the recovery of the same SGSN (for example, within the duration of 60 seconds).

  This condition occurs when the SGSN reloads and the Cisco GGSN detects it has reloaded more than once in the last 60 seconds. Stale PDP contexts do not occur if the reloads of the SGSN are more than 60 seconds apart from one another. An SGSN reloading more than once in 60 seconds is an extremely rare condition.

- CSCtf22221

  Under very rare conditions, when in a high stress and load, the Cisco GGSN might end up with stale PDP contexts after the PDP idle timer expires or occurs in combination with delete PDP context requests. This condition occurs with service-aware or Policy Charging Control (PCC)-enabled PDPs where enhanced G-CDR (eG-CDR) generation is activated.

- CSCtf29020

  The counters displayed by the **show gprs charging statistics** command are not incremented for GTP PPP type PDP contexts. This condition occurs when the charging Release 99 is configured.

- CSCtf55436

  An iSCSI session with the EMC is not reestablished on the Cisco GGSN after a session timeout.

  The condition occurs when the iSCSI connection drops because of a session timeout and a login retry is attempted.

- CSCtf56637

  When more than 200 RADIUS servers are configured, executing the **show aaa server** command on the Cisco SAMI Proxy Control Processor (PCOP) causes the Traffic and Control Plane processors (TCOPs) to crash.

- CSCtf68451

  The Cisco GGSN default behavior of dropping Transport Protocol Data Unit (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.

- CSCtf71475

  The Cisco GGSN sends CDRs even if the charging gateway sends the Xoff character in an echo request. This condition occurs with basic charging configuration.

- 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.

- CSCtf96020

  The Cisco GGSN writes extra data to the iSCSI target. This condition occurs when the GGSN has CDRS ready to be transmitted and when connectivity to the iSCSI target is restored after a failure.

- CSCtg00304

  Under high stress and load conditions (with 500 APNs and deleting PDP sessions approximately 2000 cps and above, which is equal to the rate at which the PDPs are created), the Cisco GGSN occupies the CPU at 99%, and a few sessions were unable to clear. These sessions were left as stale sessions on the GGSN. This condition impacts the serviceability to subscribers.

- 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.

- CSCtg64836

  When the TCP connection between the Cisco GGSN and the charging gateway goes down due to network issues, the GGSN writes a syslog that indicates the receipt of “CORRUPTED BYTES” from the charging gateway. This syslog should be seen only when the GGSN receives unexpected data in the TCP stream and not for the error conditions mentioned above.

  This condition occurs whenever the TCP connection between the GGSN and charging gateway goes down because of network issues.

- 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).

- CSCtg67842

  A Cisco GGSN fatal error occurs when a GTPv0 create PDP context request is received while a GTPv1 PDP creation is in progress for the same IMSI.

  This condition occurs only when the GTPv1 PDP creation is in progress (waiting for a RADIUS or Diameter server response, etc.), and the SGSN falls back to GTPv0 and sends a GTPv0 create request for the same IMSI.

- 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.

- CSCth25554

  The Cisco GGSN attempts to access a freed socket pointer for the TCP connection between the charging gateway and the GGSN when the TCP read attempt fails. This incorrect access of a freed pointer might cause memory corruption issues.

  The condition occurs when freed memory access is done when the GGSN attempts to read from the TCP socket and the read fails due to incorrect data length.

- CSCth97306

  A Cisco GGSN fatal error occurs after the GGSN transitions from standby to active.

  This fatal error occurs under the following conditions:

  1. The GGSN is functioning in prepaid standalone mode.
  2. A service-aware prepaid PDP exists.
  3. There is a PENDING CCA-U from the DCCA server and a switchover occurs.

Cisco SAMI Resolved Caveat

This section lists the Cisco SAMI caveat that is resolved in Cisco IOS Release 12.4(24)YE1.

- CSCtd17963

  During a Health-Monitoring failure in SAMI, each processor writes more than one debuginfo. Some of the debuginfos are incomplete and there will be crashinfo written in the name of debuginfo.

Other Resolved Caveats

This section lists additional miscellaneous caveats that are resolved in Cisco IOS Release 12.4(24)YE1.

- CSCte53683

  Sporadic write failures are seen while writing to an iSCSI target. This issue is seen during a race condition when the files are created and deleted from the file system.

- 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.

- CSCtf16844

  A fatal error might occur on the iSCSI IOS initiator during a SCSI command operation. The crash does not always occur, and it is due to a timing issue in the iSCSI infrastructure using NON-BLOCKING TCP write where the TCP is not able to send the packet immediately. In this scenario, the iSCSI infrastructure is not properly handling the callback from TCP.

  This condition occurs when a Small Computer System Interface (SCSI) command is sent to an iSCSI target.

- 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).

- CSCth38615

  The charging gateway status on the Traffic and Control Plane processors (TCOPs) go out of sync when one of the TCOPs receives a corrupted byte stream on the TCP connection between the GGSN and the charging gateway. While the charging gateway status is UNDEFINED in the TCOP that received the corrupted byte stream, the other TCOPs sill show its status as ACTIVE.

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

Unreproducible and Closed Caveats

This section lists caveats that have been closed or not reproduced in Cisco IOS Release 12.4(24)YE1.

- CSCte65669

  After a “High congestion threshold” alert message related to Dynamic Feedback Protocol (DFP) occurred, and when a standby GGSN was moved to active (after executing a switchover) and data was sent across approximately 800K PDP contexts, a series of malloc failures and tracebacks occurred.

  This behavior was observed only when the GGSN involved the DFP configuration, and the corresponding DFP configuration was not present on the supervisor.

- CSCte68662

  Malloc failures occur when the Cisco GGSN hits low memory threshold, and the **exec-all** command from the Proxy Control Processor (PCOP) to the Traffic and Control Plane processors (TCOPs) fails because the TCOPs cannot execute the commands due to insufficient memory.

  This condition occurs under rare and high stress conditions when there are approximately 800K PDP contexts and over one million CDR records accumulated in memory due to outage of all charging gateways.

- CSCtf32364

  When the charging path protocol set to UDP and the GTP n3 requests timer is set to 1 (instead of the default value of 5), charging gateways go down upon switchover to the standby GGSN and display as UNDEFINED in the **show gprs charging parameters** command output issued against active and standby charging gateways. The syslogs indicate that the charging path is going down on the new active GGSN because of echo request response failure.

  This condition occurs when the values of the N3 requests and T3 retransmission timers are set to 1. Effectively, this setting provides only one second of network delay to be allowed by the Cisco GGSN for the echo response before it takes down the paths to the charging gateways. This condition does not occur if the values of the N3 requests and T3 retransmission timers are left at their default values (5 and 1 respectively), and are not manually configured to lower values. The default values allow a higher delay to be tolerated by the Cisco GGSN when receiving an echo request response.

- CSCth99346

  The wrong AAA server statistics are returned when queried using SNMP. This issue is seen in Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE.

  This condition occurs when the objects of the casStatisticsTable are queried using SNMP.

- 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.

- CSCti42082

  The Cisco GGSN crashes when its interface to RADIUS is down, the SGSN restart triggers a create request with a restart counter, and the existing PDP context is deleted and a new PDP context is created.

Caveats - Cisco IOS Release 12.4(24)YE

This section contains the following types of caveats that apply to the Cisco GGSN Release 10.0, Cisco IOS Release 12.4(24)YE image:

- Open Caveats, page 38
- Resolved Caveats, page 41

Open Caveats

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

- Cisco GGSN Open Caveats, page 39
- Cisco SAMI Open Caveats, page 41
- Miscellaneous Open Caveats, page 41

Cisco GGSN Open Caveats

This section lists the GGSN-specific caveats that are open in Cisco IOS Release 12.4(24)YE:

- 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.

- CSCte56779

  A traceback is seen when the quota server interface is unconfigured. This condition occurs only when the enhance quota server interface is not enabled between the Cisco GGSN and Cisco CSG2.

  Workaround: Configure an enhanced quota server interface between the Cisco GGSN and Cisco CSG2 by specifying the **service-msg** keyword option when issuing the **ggsn quota-server** command.

- CSCte65669

  After a "High congestion threshold" alert message related to Dynamic Feedback Protocol (DFP) occurred, and when a standby GGSN was moved to active (after executing a switchover) and data was sent across approximately 800K PDP contexts, a series of malloc failures and tracebacks occurred.

  This behavior was observed only when the GGSN involved the DFP configuration, and the corresponding DFP configuration was not present on the supervisor.

  Workaround: Ensure that the corresponding DFP configuration is configured on the supervisor.

- CSCte68662

  Malloc failures occur when the Cisco GGSN hits low memory threshold, and the **exec-all** command from the Proxy Control Processor (PCOP) to the Traffic and Control Plane processors (TCOPs) fails because the TCOPs cannot execute the commands due to insufficient memory.

  This condition occurs under rare and high stress conditions when there are approximately 800K PDP contexts and over one million CDR records accumulated in memory due to outage of all charging gateways.

  Workaround: To prevent this condition from occurring, ensure secondary charging gateways are available to recover from outage of the primary gateway. Otherwise, bring up the primary gateway before the low memory threshold is reached. If bringing up a charging gateway is not possible, shut down some interfaces to free additional memory, or reload the Cisco SAMI and let the standby GGSN takeover. Reloading the module will resolve the fragmentation issue when the module comes up as the new standby GGSN. Perform another reload of the active GGSN to restore the formerly active GGSN as the active GGSN.

- CSCte97577

  The Cisco SAMI resets after the PPCs display an IXP health monitoring failure. This failure message is also present in the collected crash information. On very rare occasions, this issue might occur when thousands of sessions are initiated per second by network behind mobile subscriber (NBMS) users.

  Workaround: There is currently no known workaround.

- CSCtf04073

  PDP contexts might become stale when the Cisco GGSN receives more than one change during the recovery of the same SGSN (for example, within the duration of 60 seconds).

  This condition occurs when the SGSN reloads and the Cisco GGSN detects it has reloaded more than once in the last 60 seconds. Stale PDP contexts do not occur if the reloads of the SGSN are more than 60 seconds apart from one another. An SGSN reloading more than once in 60 seconds is an extremely rare condition.

  Workaround: There is currently no known workaround.

- CSCtf22221

  Under very rare conditions, when in a high stress and load, the Cisco GGSN might end up with stale PDP contexts after the PDP idle timer expires or occurs in combination with delete PDP context requests. This condition occurs with service-aware or Policy Charging Control (PCC)-enabled PDPs where enhanced G-CDR (eG-CDR) generation is activated.

  Workaround: There is currently no known workaround.

- CSCtf29020

  The counters displayed by the **show gprs charging statistics** command are not incremented for GTP PPP type PDP contexts. This condition occurs when the charging release 99 is configured.

  Workaround: There is currently no known workaround.

- CSCtf29044

  The Cisco GGSN does not increment the no_resource counter in the **show gprs gtp statistics** command output when a create PDP context request is rejected due to address allocation failure.

  Workaround: There is currently no known workaround.

- CSCtf32364

  When the charging path protocol set to UDP and the GTP n3 requests timer is set to 1 (instead of the default value of 5), charging gateways go down upon switchover to the standby GGSN and display as UNDEFINED in the **show gprs charging parameters** command output issued against active and standby charging gateways. The syslogs indicate that the charging path is going down on the new active GGSN because of echo request response failure.

  This condition occurs when the values of the N3 requests and T3 retransmission timers are set to 1. Effectively, this setting provides only one second of network delay to be allowed by the Cisco GGSN for the echo response before it takes down the paths to the charging gateways. This condition does not occur if the values of the N3 requests and T3 retransmission timers are left at their default values (5 and 1 respectively), and are not manually configured to lower values. The default values allow a higher delay to be tolerated by the Cisco GGSN when receiving an echo request response.

  Workaround: To bring back up the path between a charging gateway and the Cisco GGSN, send a node-alive request from each charging gateway to the Cisco GGSN once the standby GGSN transitions to the active GGSN completely (the **show gprs redundancy** command output shows the GGSN state as ACTIVE). To avoid the condition, use the default N3 requests and N3 retransmission timer values or ensure that the timers are set to a value greater than 1.

Cisco SAMI Open Caveats

There are no known caveats open in Cisco IOS Release 12.4(24)YE.

Miscellaneous Open Caveats

This section lists the Miscellaneous caveats that are open in Cisco IOS Release 12.4(24)YE.

- 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).

- 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.

  Workaround: Do not execute file create and delete operations at the same time, or ensure that the first six characters of the file names are not the same characters.

- CSCtf16844

  A fatal error might occur while when unconfiguring an iSCSI target using the **no ip iscsi target** command.

  This condition occurred when an iSCSI session was in a failed state and the user attempted to unconfigure the target.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved, or are closed or unreproducible, in Cisco IOS Release 12.4(24)YE. Only severity 1 and 2 caveats and select severity 3 caveats are listed

- Other Resolved Caveats, page 41

Other Resolved Caveats

This section lists additional miscellaneous caveats that are resolved in Cisco IOS Release 12.4(24)YE.

- 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.

- 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

- 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.

- 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.

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 43
- Platform-Specific Documents, page 44
- Cisco IOS Software Documentation Set, page 44

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 10.*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 Configuration Guide and Command Reference and associated Release Notes

  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 10.x Configuration Guide* and the *Cisco GGSN Release 10.x Command Reference* publications.