Release Notes for Cisco LTE PDN Gateway Release 1.3.7c on the Cisco SAMI, Cisco IOS Software Release 12.4 (24)T33f

Latest Publication Date: May 1, 2012, Cisco IOS Release 12.4(24)T33f
Last Publication Date: April 11, 2012, Cisco IOS Release 12.4(24)T32f

This release note describes the requirements, dependencies, and caveats for the Cisco Long Term Evolution (LTE) Packet Data Network (PDN) Gateway (PGW) Release 1.*x* 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 also apply to Cisco LTE PGW, see the "Caveats" section on page 22 and *Caveats for Cisco IOS Release 12.4 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

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

Contents

This release note includes the following information:

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

Cisco LTE PGW Overview

The following sections provide a brief overview of the Cisco LTE PGW:

LTE Evolved Packet Core

The Cisco LTE PGW is a service designed for LTE Evolved Packet Core (EPC). The EPC is the main component of the System Architecture Evolution (SAE). 3GPP designed SAE as a migration path for 3GPP systems. The SAE is the core network architecture of LTE communication and is the evolution of the General Packet Radio Service (GPRS) and Universal Mobile Telecommunication System (UMTS) that provides a migration path for 3GPP systems with the following differences:

- Simplified architecture
- All IP network
- Support for higher throughput and lower latency radio access networks (RANs)
- Support for and mobility between 3GPP (GPRS, UMTS, and LTE) and non-3GPP access technologies.

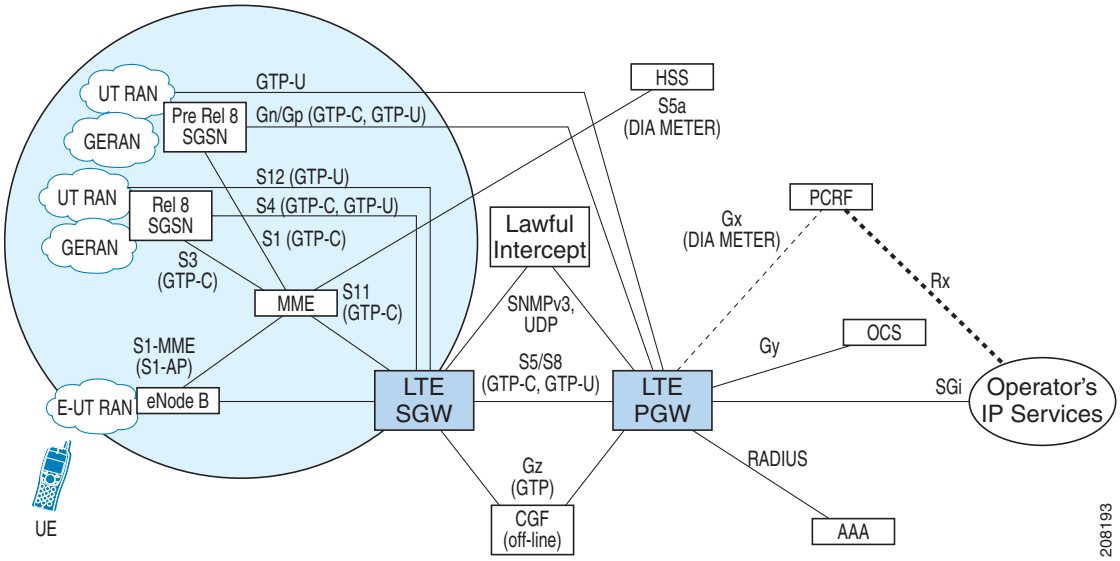
The LTE EPC is made up of the following primary elements:

- Mobility Management Entity (MME)
- Serving Gateway (SGW)
- Packet Data Network (PDN) Gateway (PGW)

Figure 1 shows the interworking (and interfaces) of the LTE EPC with different radio access technologies.

Note Cisco LTE PGW Release 1.*x* does not support the paths that appear in dashed lines.

Figure 1 LTE Network Components with SGWs and PGWs Implemented on the Cisco Service and Application Module for IP in the Cisco 7600 Series Router



The following is a list of acronyms used in Figure 1.

- Serving GPRS Support Node (SGSN)
- UMTS Terrestrial Radio Access Network (UTRAN)
- GSM EDGE Radio Access Network (GERAN)
- Evolved UTRAN (E-UTRAN)
- Mobility Management Entity (MME)
- Serving Gateway (SGW)
- PDN Gateway (PGW)
- Charging Gateway Function (CGF)
- Home Subscriber Server (HSS)
- Policy and Charging Rules Function (PCRF)
- Online Charging System (OCS)
- Authentication, Authorization, and Accounting (AAA)
- Diameter Credit Control Application (DCCA)

Cisco LTE PGW Description

For each UE associated with the EPC, there is at least one PGW providing access to the requested PDN. If a UE is accessing multiple PDNs, there could be more than one PGW for that UE.

The Cisco LTE PGW Release 1.0 and later provides the following support:

- Mobility and Roaming
  - GTP-based S5/S8 interfaces
  - Gn/Gp interface support for Pre Release 8 SGSNs
- IP Addressing and Transport
  - IP Version 4 (IPv4) and IP Version 6 (IPv6) UEs
  - IPv4 and IPv6 transport
  - Stateless Address Autoconfig (SLAAC)
  - Local pools, static IP, and RADIUS
  - Overlapping IPv4 addresses
- Authentication and Authorization
  - RADIUS AAA interface
  - RADIUS CoA and POD
  - AAA user profiles (for example, Quality of Service [QoS] and access control list [ACL])
  - AAA load balancing and failover
- Policy and QoS
  - Gx interface for Dynamic Policy and Charging Control (PCC)
  - Static (local) policies
  - Bearer level QoS parameters (QoS Class Identifier [QCI], Address Resolution Protocol [ARP], guaranteed bit rate [GBR], maximum bit rate [MBR], APN-AMBR [APN Aggregate Maximum Bit Rate])
  - Gating, rate limiting and marking
  - Call Admission Control
  - Cisco CSG2 policy interfacing
  - Enhanced PCC for CSG2
- Charging
  - GTP' offline charging
  - RADIUS off-line charging
  - Load balancing, failover, and local redirect of charging data
  - Application-based charging
  - Local storage of charging data

- Security
  - Access Control Lists (per interface, per-APN)
  - Source and destination address verification
  - Duplicate IP address protection
  - Traffic redirection
  - Virtual Routing and Forwarding (VRF)-based traffic segregation
  - Control Plane Policing
  - Security events logging
- High Reliability and Availability
  - 99.999% service availability
  - Intra- and inter-chassis session redundancy (1:1, hot standby)
  - Hot swappable components
  - In service software upgrade
  - External gateway availability monitoring
  - Manual and automatic failovers
- Overload Handling
  - Control plane throttling
  - Traps on high resource usage
  - Overload (degraded) mode of operation
- Lawful Intercept
  - Content intercept (UDP-based)
  - SNMP Version 3 based install
- Enterprise Features
  - VRF support
  - Per-enterprise authentication, authorization, and accounting
  - Enterprise-assigned IP-address
- Operation, Management, and Performance
  - Command line interface and SNMP-based management
  - SNMP Version 1, Version 2, and SNMPv3 support
  - Key performance indicators and bulk statistics
  - Subscriber and call-based tracing and logging
  - Event-based diagnostics
  - Platform and feature MIBs

The Cisco LTE PGW runs on the Cisco Service and Application Module for IP (SAMI). The Cisco SAMI is a new-generation high performance service module for the Cisco 7600 Series Router platform.

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 LTE PGW Release 1.*x* 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 LTE PGW Release 1.x

Platforms	Feature Sets	Software Image	Recommended Flash Memory (MB)	Recommended DRAM Memory (GB)	Runs From
Cisco SAMI/ Cisco 7600	PGW Standard Feature Set	c7svcsami-l3ik9s-mz	128	2	RAM

Hardware and Software Requirements

Implementing a Cisco LTE PGW Release 1.*x* and later 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 15.0(1)S or later:
  - Cisco 7600 Series Supervisor Engine 720 with a Multiplayer Switch Feature Card 3 (WS-SUP720)
  - Cisco 7600 Series Supervisor Engine 720 with a Multilayer Switch Feature Card 3 and Policy Feature Card 3B (WS-SUP720-3B)
  - Cisco 7600 Series Supervisor Engine 720 with a Multilayer Switch Feature Card 3 and Policy Feature Card 3BXL (WS-SUP720-3BXL)
  - Cisco 7600 Series Supervisor Engine 32 with a Multiplayer Switch Feature Card (WS-SUP32-GE-3B) with LCP ROMMON Version 12.2(121) or later on the Cisco SAMI.
  - Cisco 7600 Series Supervisor Engine 32 with a Multilayer Switch Feature Card and 10-Gigabit Ethernet Uplinks (WS-SUP32-10GE-3B) with LCP ROMMON Version 12.2[121] or later on the Cisco SAMI.

Or one of the following Cisco 7600 series Route Switch Processors running Cisco IOS Release 15.0(1)S 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)
- Cisco 7600 Series Route Switch Processor 720 with 10-Gigabit Ethernet Uplinks with Distributed Forwarding Card 3CXL (RSP720-3CXL-10GE)

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 15.0S*. 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 required Cisco IOS Software on the supervisor engine module depends on the supervisor engine module in use and the application running on the Cisco SAMI.

- Cisco Service and Application Module for IP (Cisco Product Number: WS-SVC-SAMI-BB-K9). The Cisco SAMI must be running Cisco IOS Release 12.4(24)T3a1 or later.

Note The Cisco LTE PGW Release 1.*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[=]).

- For security, the IPSec VPN Services Module.
- For GTP-Session Redundancy, in addition to the required hardware and software, 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.

Determining the Software Version

To determine the version of Cisco IOS Software running on your Cisco SAMI, log in to PPC3 and enter the **show version** EXEC command:

```
PGW# show version
Cisco IOS Software, SAMI Software (SAMI-L3IK9S-M), Experimental Version
12.4(20110919:095523)
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Thu 22-Sep-11 17:06 by

ROM: System Bootstrap, Version 12.4(24r)MDB, RELEASE SOFTWARE (fc1)

PGW uptime is 6 hours, 49 minutes
System returned to ROM by address error at PC 0x977A0A4, address 0x977A0A4 at 11:24:24 UTC
Thu Sep 22 2011
System restarted at 17:13:18 IST Thu Sep 22 2011

...

PGW#
```

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 view a list of MIBs supported by Cisco IOS Release 12.4(24)T33f, see the *Cisco LTE PDN Gateway Configuration Guide*.

Limitations, Restrictions, and Important Notes

When configuring the Cisco LTE PGW, note the following:

- The Cisco LTE PGW 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 redirected destination IP address and an impact to the upstream traffic flow for sessions upon bootup, ensure that you configure the **no ip cef optimize neighbor resolution** command.
- The number of bearer/PDP contexts supported on a PGW depends on the memory and platform in use and the PGW configuration; for example, whether Dynamic Feedback Protocol [DFP] is in use or the memory protection feature is enabled, and what rate of bearer creation is supported).

  Table 2 lists the maximum number the Cisco SAMI with the 2-GB memory option can support:

Table 2 Number of Bearers/PDPs Supported in 2-GB SAMI

Bearer/PDP Type	Maximum Number per SAMI
GTPv2 bearer (IPv4 and IPv6)	380,000
GTPv1 PDP (IPv4 and IPv6)	800,000

  When the maximum allowable number of bearers/PDP contexts is reached, the PGW refuses new mobile sessions until sessions are available.

- 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 HRSP interface delay before the initialization of HSRP groups with the **standby delay minimum 100 reload 100** interface configuration command.
  - To minimize issues with high CPU usage for additional reasons, disable the notification of interface data link status changes on all virtual template interfaces of the PGW using the **no logging event link-status** interface configuration command.

```
!
interface Virtual-Template1
description GGSN-VT
ip unnumbered Loopback0
encapsulation gtp
no logging event link-status
gprs access-point-list gprs
end
```

  For Mobile Express Forwarding (MEF) support, configure the **redirect all** command under the APN.

- Ensure that you configure the **radius-server source ports extended** command to enable the PGW to use 200 ports in the range from 21645 to 21844 as the source ports for sending out RADIUS requests.

New and Changed Information

The following sections list new features and behavior changes in the Cisco IOS 12.4(24)T3 releases:

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T33f

There are no new implementations or behavior changes in Cisco PGW Release 1.3.7c, Cisco IOS Release 12.4(24)T33f.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T32f

With Cisco IOS Release 12.4(24)T32f, the **show gprs gtp status** command displays the "Total initiated GTPv2 bearers" field, as seen in **bold** text in the following sample output:

```
PGW#sh gprs gtp status
GTP status:
  Total activated GTPv0 PDPs                 0
  Total activated GTPv1 PDPs                 0
  Total activated GTPv2 EPS bearers          0
  Total initiated GTPv2 bearers              0
  Total activated sessions                   0
  Total activated GTPv0 v6 PDPs              0
  Total activated GTPv1 v6 PDPs              0
  Total activated GTPv2 v6 EPS bearers       0
  Total activated IPv6 sessions              0
  Total activated GTPv1 v4v6 PDPs            0
  Total activated GTPv2 v4v6 EPS bearers     0
  Total activated IPv4v6 sessions            0
  Total activated PPP regen PDPs             0
  Total activated PPP PDPs                   0
  Total GTP direct tunnel PDPs               0
Service-aware Status:
  Prepaid PDPs                          0
  Postpaid PDPs                         0
PGW#
```

The "Total initiated GTPv2 bearers" field displays the sum of active GTPv2 bearers and the new GTPv2 session requests that are processing.

Note CSCty96931 identifies this **show gprs gtp status** command enhancement.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T31f

There are no new implementations or behavior changes in Cisco PGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T3f

Cisco LTE PGW Release 1.3.7, Cisco IOS Release 12.4(24)T3f introduces the following enhancements, new implementations, and behavior changes:

Enhanced show Command Output

The following **show** commands have been enhanced in Cisco IOS Release 12.4(24)T3f:

show gprs charging statistics

The **gprs charging statistics** command output has been enhanced to include the following charging counters:

```
Total Number of Containers sent in CDR output msgs     0
    Total Number of Services sent in CDR output msgs       0
* CDR Closed with cause
    Normal Release:                                        0
    Abnormal Release:                                      0
    Volume Limit:                                          0
    Time Limit:                                            0
    SGSN Change:                                           0
    Management Intervention:                               0
   Management Intervention Partial:                        0
    RAT Change:                                            0
    QOS Change:                                            0
    ULI Change:                                            0
    DT Change:                                             0
    Tariff Time Change:                                    0
    MS TimeZone Change:                                    0
    Container Count:                                       0
    Service Record Limit:                                  0
    Collection Timeout                                     0
    SGSN PLMN-ID Change:                                   0
    SGSN and PLMN-ID Change:                               0
```

Note CSCts68540 identifies this **show** command enhancement.

show tech

The **show tech** command has been enhanced to include output for the **show ip traffic** command and the **show sctp statistics** command. Additionally, "dma controller statistics" are collected as part of the **show platform** command and displayed in the enhanced **show tech** command output.

Note CSCtt00301 identifies this **show tech** command enhancement.

show gprs gtp statistics

The **show gprs gtp statistics** command output has been enhanced to include the following QoS counters (in bold) in the Debug info section:

```
Debug info:
  Path fail local del PDP        1208633616 Ver upgrade local del          0
  No SGSN/SGW local del PDP      0          Ver fallback local del         0
  No wait SGSN/SGW local del PDP 0          No req SGSN/SGW local del PDP  0
  Create collide with delete     0          Version changes                0
  Rcvd retransmit create req     0          Create as update               2
  Del recd for del session       0          Incorrect Ref Count State      0
  Total v2 restart txn tmr expiry      19
  v2 restart txn exp with no PDP       0
  v2 restart txn exp with not v2 PDP   0
  Restart txn cancelled for other proc 0
  CoA delayed for retry                19
  Max backoff retries failed           1
  Create session req reassign    0
```

Table 3 describes the new fields.

Table 3 New show gprs gtp statistics Command Field Descriptions

Field	Description
Total v2 restart txn tmr expiry	Number of times the GTPv2 backoff restart timer has expired.
v2 restart txn exp with no PDP	Number of PDPs that were deleted while running the backoff timer.
v2 restart txn exp with not v2 PDP	Number of PDPs no longer GTPv2 PDPs when the backoff time has expired.
Restart txn cancelled for other proc	Number of times the backoff timer has restarted for a reason other than collision.
CoA delayed for retry	Number of times CoA has been delayed because a PDP update failed with collision.
Max backoff retries failed	Number of times the maximum backoff retries has failed.

Note CSCtt41315 identifies this **show gprs gtp statistics** command enhancement.

Lookup Thread Health Monitoring

The Cisco SAMI IXP has more than 50 lookup threads. In prior releases, if a few threads failed, the system did not report the failure right away, but continued to operate in a degraded mode.

Cisco IOS Release 12.4(24)T3f introduces a new mechanism that monitors the health of the lookup threads every second to ensure that the threads are functioning properly. If eight threads report a failure, the mechanism resets the system.

The following syslog message is printed to the PPC if the monitor mechanism detects a stuck thread:

```
SAMI 3/3: Oct 28 07:22:57.771: %PLATFORM-3-DP_IXP_THR_WARN: IXP:0 thread blocked. me:10
thr:7 num_consecutive_fail:3
```

Once eight threads become stuck, the monitor mechanism prints the following syslog message and reloads the card:

```
SAMI 3/3: Oct 28 07:22:57.771: %PLATFORM-0-DP_IXP_MULT_THR_FAIL: IXP:0 multiple:8 threads
hung
```

By default, the lookup thread monitor mechanism is enabled for both Cisco SAMI IXPs. To disable the monitor mechanism, use the **no sami ixp monitor enable** command. To reenable the monitor mechanism, use the **sami ixp monitor enable** command.

Note CSCtt32257 identifies this new implementation.

Write Memory Command Disabled on the TCOPs

With Cisco IOS Release 12.4(24)T3f, the **write memory** command is disabled on the Cisco SAMI Traffic and Control Plane processors (TCOPs). Disabling the **write memory** command on the TCOPs prevents unnecessary and redundant writes to NVRAM that previously occurred when using schedule jobs (cron table jobs) that executed the **write memory** command.

Note This behavior change fixes CSCtt37393.

SNMP Changes

In the CISCO-GGSN-EXT-MIB, the SNMP GetNext (snmpgetnext, snmpwalk) and the SNMP GetBulk (snmpbulkget) requests are disabled for the GGSN Subscriber table (cGgsnExtSubscriberTable). The entries of the GGSN Subscriber table are now available only through an SNMP GetOne request (snmpget).

Note This behavior change resolves CSCtt71202.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T3e

Cisco LTE PGW Release 1.3.6 introduces support for the following:

- Displaying Enhanced Service Control Message Statistics, page 14
- Throttling GTP Request Reenqueues, page 16
- Clearing Bearer/PDP Sessions on a TCOP, page 17

Restart Counter Change Syslog Message

Cisco LTE PGW Release 1.3.6 introduces the following syslog messages, which indicate that a restart counter change has occurred that caused an SGSN/SGW to reload and deleted all of the contexts linked to that SGSN/SGW.

```
SAMI 4/5: 000686: Nov 14 00:36:47: %GTP-4-RESTART_COUNTER_CHANGED: GSN: 198.228.216.76,
Sig src addr: 135.211.6.144, TID: 1340019236686654, SGSN 135.211.6.144 Restart counter
changed from 74 to 75,  -Traceback= 0x44307C18z 0x442FCAA0z 0x442FD85Cz 0x45990878z
0x45993F7Cz

SAMI 3/4: %LTE_GTPV2-4-LTE_RESTART_COUNTER_CHANGED: GSN: 6.6.6.1, Sig src addr:
12.12.12.36, TID: 1111051000000021, SGW: 12.12.12.36 Restart counter changed from 10 to 2,
-Traceback= 0x9DC6904z 0x9E65E24z 0x9E948F4z 0x9E91804z 0x9E1CB2Cz 0xA279560z 0xA2795D0z
0x9E16654z 0x9E91584z 0x9E808A4z 0x9E88EECz 0x9E93F3Cz 0x830D7C0z 0x99C1DB8z 0x99C54BCz
```

Where,

- GSN—IP address of the GGSN.
- Sig src address—Source signaling address of the message that indicates the restart counter change.
- TID—Tunnel Identifier (TID) of the context for which the signaling message is received.
- SGSN—IP address of the SGSN.
- SGW—IP address of the SGW.
- Restart counter changed from *x* to *y*—Old and new restart count.

The traceback is harmless and associated with the syslog message.

Displaying Enhanced Service Control Message Statistics

With Cisco LTE PGW Release 1.3.6, the **show ggsn csg statistics** command supports a **detailed** keyword option that enables operators to display detailed service usage message processing on the quota server interface.

To display additional information about the service control requests (SCRs) and service control usage (SCU) messages that the PGW exchanges with the Cisco CSG2 on the quota server interface, use the following command while in privileged EXEC mode and specify the **detailed** keyword option:

Command	Purpose
`Router# show ggsn csg statistics [detailed]`	Displays detailed information about the service control messages exchanged on the quota server interface.

Example 1

The following is the output for the **show ggsn csg statistics** command with the **detailed** keyword option specified. The additional fields that display when you specify the detailed keyword option are in **bold** text.

```
PGW# show ggsn csg statistics detailed
GGSN CSG path statistics:
CSG Group Name:   csg2
 CSG Path statistics:
  Outbound msg count:   967
  Outbound byte count:  6760
  Inbound msg count:    966
  Inbound byte count:   6770
 CSG Path msg statistics:
  Service Auth Req:     0
  Service Auth Resp:    0
  Service Reauth Req:   0
  Quota Return:         0
  Quota Return Req:     0
  Quota Return Accept:  0
  Service Stop:         0
  Service Stop Req:     0
  Quota Push:           0
  Quota Push resp:      0
  GTP' Acks:            0

 Service Control Message Statistics:
  Service Control Req:                    0
      Total sent:                   0           Retransmits:    0
  Enhanced Radius Interim msg:            0
  Enhanced Radius Stop msg:               0
  Service Control Req Ack:                0
      Immediate:                    0           Delayed:        0
  Service Control Req Nack:               0
      Immediate:                    0           Delayed:        0
  Service Control Usage:                  0
      Parse errors:                 0           Invalid user:   0
      No user:                      0           Internal fail:  0
      Usage outside upper seq win:  0
      Usage outside lower seq win:  0
  Sync Service Control Usage:             0
      No matching req:              0       Processing error:  0
  Async Service Control Usage:            0
      No service info:              0       Processing error:  0
  Service Control Usage Ack:              0
  Service Control Usage Nack:             0
  Expected sequence SCU msgs:             0
      Async msgs:                   0
        Svc Records added:          0           Failed:         0
      Sync msgs for SCR:            0
        Svc Records added:          0           Failed:         0
      Sync msgs for radius interim: 0
        Svc Records added:          0           Failed:         0
      Sync msgs for radius stop:    0
        Svc Records added:          0           Failed:         0
  Out of order sequence msgs:             0
      Async msgs:                   0
      Sync msgs for SCR:            0
      Sync msgs for radius interim: 0
      Sync msgs for radius stop:    0
  Out of order msgs processed:            0
      Async msgs:                   0
        Svc Records added:          0           Failed:         0
```

```
    Sync msgs for SCR:              0
      Svc Records added:            0             Failed:          0
    Sync msgs for radius interim:   0
      Svc Records added:            0             Failed:          0
    Sync msgs for radius stop:      0
      Svc Records added:            0             Failed:          0
    On process all:                 0             On usage:        0
    User Sequence skips:            0
  User sequence window slides:              0
    Attempts:                       0             User Seq skips: 0
  User sequence window wraps:               0
  No SCU recd:                              0
    For service control req:        0
    For enhanced radius interim:    0
    For enhanced radius stop:       0
  SCR fail to send:                         0
  No Ack for SCR:                           0
  Enhanced Radius Interim msg fail to send: 0
  Enhanced Radius Stop msg fail to send:    0
  SCR correlation skips on peer:            0

PGW#
```

Note This new implementation is identified by CSCtr20034.

Throttling GTP Request Reenqueues

If there is a GTP request that the PGW must service for an existing bearer/PDP, and a pending request for that bearer/PDP exists, the PGW cannot immediately service the new request.

In some cases the GTP request is reenqueued in the GTP queue until the bearer/PDP is ready to be updated/created. The PGW should service all such GTP requests within a few reenqueues. If for some reason it cannot, and a request is continuously reenqueued, the PGW attempts to process the same request again and again, which causes a high CPU.

With Cisco LTE PGW Release 1.3.6, you can throttle the number of times a GTP request can be reenqueued.

To configure the number of times a GTP request can be reenqueued 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 from 1 through 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 bearers/PDPs, and the command is immediately effective.

To display reenqueue 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:

```
PGW# 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
PGW#
```

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 reenqueue statistics.

When configuring the GTP request reenqueue throttle, note the following:

- When **debug gprs gtp errors** is enabled, the following debug messages display if a GTP request is reenqueued for the configured or default value:

  ```
  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.

Note CSCtr30916 identifies this new implementation.

Clearing Bearer/PDP Sessions on a TCOP

From the Cisco SAMI Remote Console and Logging (RCAL) interface, use the **execute-on** command while in privileged EXEC mode from the PCOP to collect and display **show** and **debug** command output from the TCOPs. Additionally, use the **execute-on** command to propagate most **clear** commands to the TCOPs.

With Cisco PGW Release 1.3.6, the **clear gprs gtp pdp-context** command supports clearing a specific number of sessions on a TCOP. This enhancement enables operators to implement controlled bearer/PDP flushes.

To clear a specific number of bearer/PDP sessions on a TCOP, use the following command while in privileged EXEC mode:

Command	Purpose
`Router# execute-on` *tcop-num* `clear gprs gtp pdp-context` *count*	Clears the specified number of bearers/PDPs from a TCOP, where: • *tcop-num*—Name of the TCOP from which you want to clear bearers/PDPs. • *count*—Number of bearers/PDPs you want to clear from the TCOP. A valid value is a number from 1 through 160000. **Note** You cannot execute the **clear gprs gtp pdp-context** command and specify the *clear* variable directly on the PCOP.

Note CSCts43204 identifies this new implementation.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T35c

There are no new implementations or behavior changes in Cisco PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T34d

There are no new implementations or behavior changes in Cisco PGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T3c

Cisco LTE PGW Release 1.3 introduces support for the following PCO options:

- P-CSCF Address Request
- IPv4 (0x0C) and IPv6 (0x01)
- IPv4 DNS (0x03) and IPv6 DNS (0x0D)
- Address Allocation from NAS (0x0A)
- DHCPv4 (0x08)

Note This new implementation is identified by CSCts43204.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T3b

Per CR 225, with Cisco LTE PGW Release 1.2, the Tracking Area Identity (TAI) and User Location Information (ECGI) are included in the change report action information element (IE), according to the received event trigger, in the following messages:

- Create Session Response
- Create Bearer Request
- Modify Bearer Response
- Update Bearer Request
- Change Notification Response

Note This new implementation is identified by CSCth92541.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T3a1

The following new feature and compliance change have been introduced in Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1:

- Configuring Local Service Record Information Generation, page 19
- Configuring Specification Compliance, page 20

Configuring Local Service Record Information Generation

By default, the Cisco LTE PGW obtains service record information from the Cisco CSG2. With Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1, service record information can be generated locally, without the Cisco CSG2.

Service Record Generation with a Cisco CSG2

When generating service record information with a Cisco CSG2, the following configuration must exist:

- Service aware billing is enabled on the APN using the **service-aware** access-point configuration command.
- The charging record type is set to **pcdr** using the **charging record type** access-point configuration command.
- Traffic is redirected to the Cisco CSG2 using the **redirect all** access-point configuration command.

With the service record generation with a Cisco CSG2 implementation, the Cisco CSG2 sends the service record information to the Cisco LTE PGW, which then adds it to the CDR.

Service Record Generation without a Cisco CSG2

When generating service record information without a Cisco CSG2, the following configuration must exist:

- Service aware billing is not enabled on the APN.
- The charging record type is set to **pcdr** using the **charging record type** access-point configuration command.
- Traffic is redirected directly to the Gi interface using the **redirect all** access-point configuration command.

With the service record without a Cisco CSG2 implementation, the PGW generates the service information and adds it to the CDR.

Note Service record information added by the PGW for non service aware APNs does not include information for the following fields, which are defined as optional by the 3GPP specifications: time of last usage, time of last usage, and time usage.

To enable the PGW to generate service record information locally, complete the following tasks while in charging profile configuration mode.

Command	Purpose
`Router(ch-prof-conf)# service id num`	Configures the default service identifier for the service record information locally generated and added to the P-CDR by the PGW. The service identifier is used to identify the service or the service component to which the service data flow relates. (See Service-Identifier AVP as defined in TS 29.212.) A valid value is a number from 1 through 4294967295. The default is 1.
`Router(ch-prof-conf)# rating id num`	Configures the default IP service flow identity. (See Rating-Group AVP as defined in TS 32.299.) A valid value is a number from 1 through 4294967295. The default is 1.

Note For more information about configuring charging profiles, see the *Cisco LTE PGW Configuration Guide*.

Configuring Specification Compliance

Support for the following 3GPP specification change requests (CRs) records for 29.274 has been introduced in Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1:

- CR 267—Serving Network
- CR 358—Bearer QoS in modify bearer request
- CR 430—UE Timezone and user location information (ULI) included in bearer response messages
- CR 433—Correcting misaligned information element (IE) presence type statements

- CR 451—Charging characteristics value for active PDN connections
- CR 154—Offending IE in the cause IE

Additionally, commands to configure backward compliance have been added for the following 29.274 CRs:

- CR 308—LBI clarifications for Gn/Gp handovers. By default, compliance for this CR 308 is enabled on the PGW, but by default is disabled on the SGW.
- CR 324—APN-AMBR in the create/delete bearer request. Compliance must be enabled on the PGW and SGW. By default, compliance for this CR is disabled.
- CR 137—Combined uplink and downlink traffic flow template (TFT) IEs. CR 137 Compliance must be enabled on the PGW and SGW. By default, compliance for CR 137 is disabled.

To configure compliance for the above CR, complete the following tasks:

- Creating a Compliance Profile, page 21
- Creating a Remote Path Group, page 22

Creating a Compliance Profile

Operators can create a compliance profile in which they configure CR compliance. Once a compliance profile has been created, it can be applied to a path group to a remote node. For information on creating a path group to a remote node, see"Creating a Remote Path Group" section on page 22.

To create a compliance profile and its CR configuration, complete the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs compliance profile name`	Creates or modifies a compliance profile, where *name* is the name of the compliance profile.
Step 2	`Router(config-compl-profile)# cr 29.274-0308`	Configures the gateway to comply with CR 308 (LBI clarifications for Gn/Gp handovers). On the PGW, CR 308 compliance is enabled by default. On the SGW, compliance is disabled by default.
Step 3	`Router(config-compl-profile)# cr 29.274-0324`	Configures the gateway to comply with CR 324 (APN AMBR in the create/delete bearer request). On the PGW and SGW, CR 324 compliance is disabled by default.
Step 4	`Router(config-compl-profile)# cr 29.274-0137`	Configures the gateway to comply with CR 137 (combine uplink and downlink TFT IEs). On the PGW and SGW, compliance is disabled by default.

Creating a Remote Path Group

Once a compliance profile has been configured, operators can create a path group. In the path group, the address of the remote node is configured and as well as the compliance profile to use.

To create a path group, complete the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs remote group name`	Creates or modifies a remote path group, where *name* is the name of the group.
Step 2	`Router(config-remote-group)# compliance name`	Applies a preconfigured compliance profile to the path group.
Step 3	`Router(config-remote-group)# ip address {v4 start_ipv4_addr end_ipv4_addr | v6 start_ipv6_addr end_ipv6_addr}`	Configures an IP address range in the remote path group, where: • **v4** *start_ipv4_addr end_ipv4_addr*—IPv4 address range. • **v6** *start_ipv6_addr end_ipv6_addr*—IPv6 address range.

Caveats

This section contains the caveats for the following releases:

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)T33f.

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.

Note To display a list of caveats for Cisco IOS Release 12.4(24)T33f, on the Bug Toolkit page, use the **Software Version** drop down lists to select Cisco IOS Version 12.4(24)T33f. To display information about a specific caveat, type the caveat number in the **Search for Bug ID** field.

Caveats - Cisco LTE PGW Release 1.3.7c, Cisco IOS Release 12.4(24)T33f

This section lists the open, resolved and unreproducible caveats that pertain to Cisco LTE PGW Release 1.3.7c, Cisco IOS Release 12.4(24)T33f.

- Open Caveats, page 23
- Resolved Caveats, page 27

Open Caveats

Note Caveats open in one 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 LTE PGW Caveats, page 23
- Cisco SAMI Caveats, page 26

Cisco LTE PGW Caveats

The following Cisco LTE PGW caveats are open in Cisco IOS Release 12.4(24)T33f.

- CSCtj25287

  During the creation of a session, if a failure response from the IXP occurs while the session is being deleted under a specific timing window (for example, the IXP might already have an entry), the PGW might reload.

  This is a timing condition between the completion of accounting start and the deletion of a session under a specific timing window.

  Workaround: There is currently no known workaround.

- CSCts34338

  The Cisco LTE PGW/SGW might drop an update PDP context requests because of an International Mobile Subscriber Identity (IMSI) mandatory information element (IE) missing error. This condition occurs during a GTPv0-to-GTPv1 handoff or during a GTPv2-to-GTPv1 handoff if the IMSI is not present in the update PDP context request. The PGW/SGW considers this a mandatory IE instead of an optional ID, and drops the incoming request.

  Workaround: There is currently no known workaround.

- CSCts90790

  Not all GTPv1 PDPs are cleared on newly active PGW when the restart counter is changed and a failover occurs at the same time.

  Workaround: There is currently no known workaround.

CSCtt11538

Incorrect values for APN counters display when a PDP is reassigned to a different Traffic and Control Plane processor (TCOP).

This condition occurs only when a PDP is reassigned to a different TCOP.

Workaround: There is currently no known workaround.

- CSCtu10175

  The following syslog message might seen:

  ```
  %IPC-3-SAMI_SM_FAIL_DUP_MSISDN: Unexpected condition: TCOP in IMSI-Sticky doesn't
  match with MSISDN-Sticky.
  ```

  This message might be seen with one of the following:

  a. Inter RAT handoff from UTRAN to E-UTRAN (GTPv1-to-GTPv2 handoff) occurs, if a create session request is received on the SGW without an MSISDN IE, or

  b. TCOP reassignment happens during create-over-create scenario, because the new create request fails on the TCOP where the session exists.

  The message does not appear to impact any functionality.

  Workaround: There is currently no known workaround.

- CSCtu24144

  When polling of cGgsnExtSubscriberTable for GTPv2 calls, the trailing zeros of mobile station ISDNs (MSISDNs) are ignored.

  When there are calls whose MSISDN has trailing zeros, **snmpget** appears to function properly, even if the zeros are omitted, as seen in the following example command output:

```
pgw-03#show gprs gtp pdp-context msisdn
TID              MS Addr      Source  SGW Addr        SGSN Addr       MSISDN             APN
2233445566110010 10.0.3.230   LOCAL   111.111.111.13  N/A             2233445566110000   broadband
```

  Although there is only one session, the following **snmpget** returns same value:

```
snmpget -v 2c 130.130.0.10 -c abc cGgsnExtSubscriberTid.12.50.50.51.51.52.52.53.53.54.54.49.49
CISCO-GGSN-EXT-MIB::cGgsnExtSubscriberTid."223344556611" = STRING: 2233445566110010

snmpget -v 2c 130.130.0.10 -c abc cGgsnExtSubscriberTid.14.50.50.51.51.52.52.53.53.54.54.49.49.48.48
CISCO-GGSN-EXT-MIB::cGgsnExtSubscriberTid."22334455661100" = STRING: 2233445566110010

snmpget -v 2c 130.130.0.10 -c abc
cGgsnExtSubscriberTid.16.50.50.51.51.52.52.53.53.54.54.49.49.48.48.48.48
CISCO-GGSN-EXT-MIB::cGgsnExtSubscriberTid."2233445566110000" = STRING: 2233445566110010
```

  Workaround: Ensure that the scenario like below does not occur (two calls with the same MSISDN, minus two trailing zeros at the end of one):

```
pgw-03#show gprs gtp pdp-context msisdn
TID              MS Addr      Source  SGW Addr        SGSN Addr       MSISDN             APN
2233445566110010 10.0.3.230   LOCAL   111.111.111.13  N/A             2233445566110000   broadband
9933445566113314 10.0.3.250   LOCAL   111.111.111.13  N/A             22334455661100     broadband
```

- CSCtu35882

  Negative values for global and path statistics are retrieved by the Mobile Wireless Transport Manager (MWTM) when polling standby gateway.

  This condition occurs when the MWTM polls the GTP-MIB and the GTPv2-MIB on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCtu41869

  Spurious memory access tracebacks are observed when a GTPv2 session is handed off to a GTPv1 PDP while the session is waiting for an update bearer response. While a traceback is observed, the GTPv2-to-GTPv1 handoff is successful and no impact to functionality is observed.

  This condition occurs only when a GTPv2-to-GTPv1 handoff is occurring while the GTPv2 session is waiting for an update bearer response.

  Workaround: There is currently no known workaround.

- CSCtu51795

  There are no counters present to verify the drops from pending_requestQ per PDP.

  A maximum of 16 PDPs can be queued for processing. Currently, there are no counters to check the current status of the queue, and to see if any messages are dropped from the queue.

  Workaround: There is currently no known workaround.

- CSCtw47142

  The Cisco LTE gateways print the following error message to the console if they receive a Version Not Supported message from the charging gateway.

```
 %GTP-0-CORRUPTED_GTP_BYTE_STREAM: Corrupted byte stream, GSN: 172.16.57.15, Closing
socket
 %GTP-0-PACKETPARSINGERROR: GSN: 172.16.78.83, TID: 00, APN: NULL, Reason: LFN in CHRG
msg should be set
 %GTP-0-PACKETPARSINGERROR: GSN: 172.16.57.15, TID: 00, APN: NULL, Reason: Unexpected
message 0x1A
```

  This condition occurs because the Cisco LTE gateways are unable to parse the Version Not Supported packet. The TCP connection between LTE gateways and the charging gateway is re-established to recover from this condition.

  Workaround: There is currently no known workaround.

- CSCtw50105

  The Cisco Mobile Wireless Transport Manager (MWTM) is unable to scale with the number of entries provided by the GTPv2 MIB path table.

  This condition occurs when GTPv2 reporting is enabled on the MWTM.

  Workaround: Disable GTPv2 reporting on the MWTM.

- CSCtw63171

  The primary charging gateway is active on the Proxy Control Processor (PCOP) and the secondary charging gateway is active on the Traffic and Control Plane processors (TCOPs).

  This condition occurs when the Version Not Support message is received on the gateway PCOP.

  Workaround: The workaround for this condition is present in the code. The PCOP detects the mismatch of charging gateways on different processors and disconnects and reestablishes the TCP connection with the primary charging gateway.

- CSCtz20397

  The standby PGW might not update session QoS correctly after a policy control and charging rules function (PCRF) Re-Auth-Request (RAR).

  This condition occurs only when the PGW receives an update bearer request due to a PCRF RAR and a modify bearer request from an SGW due to a UE X2 handoff at the same time. If the messages are received sequentially with proper responses, the condition does not occur.

  Workaround: There is currently no known workaround.

Cisco SAMI Caveats

The following Cisco SAMI caveats are open with Cisco IOS Release 12.4(24)T33f.

- CSCtn88798

  In a redundant implementation, one of the Cisco SAMIs remains in a STANDBY-COLD state indefinitely. When in a STANDBY-COLD state, sessions are not sychronized to the standby Cisco SAMI.

  This condition is seen on occasions when both of the Cisco SAMIs that are a part of a redundant implementation are reloaded at very close times.

  Workaround: Reload the Cisco SAMI that is in STANDBY-COLD state.

- CSCts50055

  On rare occasions, a Cisco SAMI coming up as a standby (in a redundant implementation) reloads immediately after booting up because of IXP network processor health monitoring failures.

  These IXP health monitoring failures are only seen on Cisco SAMIs coming up as the standby gateway in a redundant implementation.

  Workaround: The Cisco SAMI reloads correctly on its own on the next attempt.

- CSCtu50827

  The Cisco SAMI reloads due to an LCP-to-PPC health monitoring failure.

  This reload occurs only when the very rare condition of a flash operation happening at the same time a software issues causes a crash.

  Workaround: There is currently no known workaround.

- CSCtu73030

  The Cisco SAMI reboots with following logs displaying at the supervisor console:

  ```
  Card in module slot_num, is being power-cycled off (Module not responding to Keep
  Alive polling)
  ```

  After the reload, the dir core: in LCP does not contain any logs that indicate the reason for the reload.

  It is not clear what conditions trigger this error since there were no specific activities going through the LCP at the time the reload occurred.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list the caveats that have been resolved in Cisco LTE PGW Release 1.3.7c, Cisco IOS Release 12.4(24)T33f.

- Cisco LTE PGW Caveats, page 27
- Cisco SAMI Caveats, page 27

Cisco LTE PGW Caveats

There are no Cisco LTE PGW caveats newly resolved with Cisco LTE PGW Release 1.3.7c, Cisco IOS Release 12.4(24)T33f.

Cisco SAMI Caveats

There are no Cisco SAMI caveats newly resolved with Cisco LTE PGW Release 1.3.7c, Cisco IOS Release 12.4(24)T33f.

Caveats - Cisco LTE PGW Release 1.3.7b, Cisco IOS Release 12.4(24)T32f

This section lists the open, resolved and unreproducible caveats that pertain to Cisco LTE PGW Release 1.3.7b, Cisco IOS Release 12.4(24)T32f.

- Open Caveats, page 34
- Resolved Caveats, page 38
- Unreproducible Caveats, page 33

Open Caveats

Note Caveats open in one 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 LTE PGW Caveats, page 34
- Cisco SAMI Caveats, page 37

Cisco LTE PGW Caveats

The following Cisco LTE PGW caveats are open in Cisco IOS Release 12.4(24)T32f.

- CSCtj25287

  During the creation of a session, if a failure response from the IXP occurs while the session is being deleted under a specific timing window (for example, the IXP might already have an entry), the PGW might reload.

  This is a timing condition between the completion of accounting start and the deletion of a session under a specific timing window.

  Workaround: There is currently no known workaround.

- CSCts34338

  The Cisco LTE PGW/SGW might drop an update PDP context requests because of an International Mobile Subscriber Identity (IMSI) mandatory information element (IE) missing error. This condition occurs during a GTPv0-to-GTPv1 handoff or during a GTPv2-to-GTPv1 handoff if the IMSI is not present in the update PDP context request. The PGW/SGW considers this a mandatory IE instead of an optional ID, and drops the incoming request.

  Workaround: There is currently no known workaround.

- CSCts90790

  Not all GTPv1 PDPs are cleared on newly active PGW when the restart counter is changed and a failover occurs at the same time.

  Workaround: There is currently no known workaround.

- CSCtt11538

  Incorrect values for APN counters display when a PDP is reassigned to a different Traffic and Control Plane processor (TCOP).

  This condition occurs only when a PDP is reassigned to a different TCOP.

  Workaround: There is currently no known workaround.

- CSCtu10175

  The following syslog message might seen:

  ```
  %IPC-3-SAMI_SM_FAIL_DUP_MSISDN: Unexpected condition: TCOP in IMSI-Sticky doesn't
  match with MSISDN-Sticky.
  ```

  This message might be seen with one of the following:

  a. Inter RAT handoff from UTRAN to E-UTRAN (GTPv1-to-GTPv2 handoff) occurs, if a create session request is received on the SGW without an MSISDN IE, or

  b. TCOP reassignment happens during create-over-create scenario, because the new create request fails on the TCOP where the session exists.

  The message does not appear to impact any functionality.

  Workaround: There is currently no known workaround.

- CSCtu24144

  When polling of cGgsnExtSubscriberTable for GTPv2 calls, the trailing zeros of mobile station ISDNs (MSISDNs) are ignored.

  When there are calls whose MSISDN has trailing zeros, **snmpget** appears to function properly, even if the zeros are omitted, as seen in the following example command output:

```
pgw-03#show gprs gtp pdp-context msisdn
TID              MS Addr      Source  SGW Addr        SGSN Addr       MSISDN              APN
2233445566110010 10.0.3.230   LOCAL   111.111.111.13  N/A             2233445566110000    broadband
```

  Although there is only one session, the following **snmpget** returns same value:

```
snmpget -v 2c 130.130.0.10 -c abc cGgsnExtSubscriberTid.12.50.50.51.51.52.52.53.53.54.54.49.49
CISCO-GGSN-EXT-MIB::cGgsnExtSubscriberTid."223344556611" = STRING: 2233445566110010

snmpget -v 2c 130.130.0.10 -c abc cGgsnExtSubscriberTid.14.50.50.51.51.52.52.53.53.54.54.49.49.48.48
CISCO-GGSN-EXT-MIB::cGgsnExtSubscriberTid."22334455661100" = STRING: 2233445566110010

snmpget -v 2c 130.130.0.10 -c abc
cGgsnExtSubscriberTid.16.50.50.51.51.52.52.53.53.54.54.49.49.48.48.48.48
CISCO-GGSN-EXT-MIB::cGgsnExtSubscriberTid."2233445566110000" = STRING: 2233445566110010
```

  Workaround: Ensure that the scenario like below does not occur (two calls with the same MSISDN, minus two trailing zeros at the end of one):

```
pgw-03#show gprs gtp pdp-context msisdn
TID              MS Addr      Source  SGW Addr        SGSN Addr       MSISDN              APN
2233445566110010 10.0.3.230   LOCAL   111.111.111.13  N/A             2233445566110000    broadband
9933445566113314 10.0.3.250   LOCAL   111.111.111.13  N/A             22334455661100      broadband
```

- CSCtu35882

  Negative values for global and path statistics are retrieved by the Mobile Wireless Transport Manager (MWTM) when polling standby gateway.

  This condition occurs when the MWTM polls the GTP-MIB and the GTPv2-MIB on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCtu41869

  Spurious memory access tracebacks are observed when a GTPv2 session is handed off to a GTPv1 PDP while the session is waiting for an update bearer response. While a traceback is observed, the GTPv2-to-GTPv1 handoff is successful and no impact to functionality is observed.

  This condition occurs only when a GTPv2-to-GTPv1 handoff is occurring while the GTPv2 session is waiting for an update bearer response.

  Workaround: There is currently no known workaround.

- CSCtu51795

  There are no counters present to verify the drops from pending_requestQ per PDP.

  A maximum of 16 PDPs can be queued for processing. Currently, there are no counters to check the current status of the queue, and to see if any messages are dropped from the queue.

  Workaround: There is currently no known workaround.

- CSCtw47142

  The Cisco LTE gateways print the following error message to the console if they receive a Version Not Supported message from the charging gateway.

```
 %GTP-0-CORRUPTED_GTP_BYTE_STREAM: Corrupted byte stream, GSN: 172.16.57.15, Closing
socket
 %GTP-0-PACKETPARSINGERROR: GSN: 172.16.78.83, TID: 00, APN: NULL, Reason: LFN in CHRG
msg should be set
 %GTP-0-PACKETPARSINGERROR: GSN: 172.16.57.15, TID: 00, APN: NULL, Reason: Unexpected
message 0x1A
```

  This condition occurs because the Cisco LTE gateways are unable to parse the Version Not Supported packet. The TCP connection between LTE gateways and the charging gateway is re-established to recover from this condition.

  Workaround: There is currently no known workaround.

- CSCtw50105

  The Cisco Mobile Wireless Transport Manager (MWTM) is unable to scale with the number of entries provided by the GTPv2 MIB path table.

  This condition occurs when GTPv2 reporting is enabled on the MWTM.

  Workaround: Disable GTPv2 reporting on the MWTM.

- CSCtw63171

  The primary charging gateway is active on the Proxy Control Processor (PCOP) and the secondary charging gateway is active on the Traffic and Control Plane processors (TCOPs).

  This condition occurs when the Version Not Support message is received on the gateway PCOP.

  Workaround: The workaround for this condition is present in the code. The PCOP detects the mismatch of charging gateways on different processors and disconnects and reestablishes the TCP connection with the primary charging gateway.

- CSCtz20397

  The standby PGW might not update session QoS correctly after a policy control and charging rules function (PCRF) Re-Auth-Request (RAR).

  This condition occurs only when the PGW receives an update bearer request due to a PCRF RAR and a modify bearer request from an SGW due to a UE X2 handoff at the same time. If the messages are received sequentially with proper responses, the condition does not occur.

  Workaround: There is currently no known workaround.

Cisco SAMI Caveats

The following Cisco SAMI caveats are open with Cisco IOS Release 12.4(24)T32f.

- CSCtn88798

  In a redundant implementation, one of the Cisco SAMIs remains in a STANDBY-COLD state indefinitely. When in a STANDBY-COLD state, sessions are not sychronized to the standby Cisco SAMI.

  This condition is seen on occasions when both of the Cisco SAMIs that are a part of a redundant implementation are reloaded at very close times.

  Workaround: Reload the Cisco SAMI that is in STANDBY-COLD state.

- CSCts50055

  On rare occasions, a Cisco SAMI coming up as a standby (in a redundant implementation) reloads immediately after booting up because of IXP network processor health monitoring failures.

  These IXP health monitoring failures are only seen on Cisco SAMIs coming up as the standby gateway in a redundant implementation.

  Workaround: The Cisco SAMI reloads correctly on its own on the next attempt.

- CSCtu50827

  The Cisco SAMI reloads due to an LCP-to-PPC health monitoring failure.

  This reload occurs only when the very rare condition of a flash operation happening at the same time a software issues causes a crash.

  Workaround: There is currently no known workaround.

- CSCtu73030

  The Cisco SAMI reboots with following logs displaying at the supervisor console:

  ```
  Card in module slot_num, is being power-cycled off (Module not responding to Keep
  Alive polling)
  ```

  After the reload, the dir core: in LCP does not contain any logs that indicate the reason for the reload.

  It is not clear what conditions trigger this error since there were no specific activities going through the LCP at the time the reload occurred.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list the caveats that have been resolved in Cisco LTE PGW Release 1.3.7b, Cisco IOS Release 12.4(24)T32f.

Cisco LTE PGW Caveats

The following PGW caveats are resolved in Cisco IOS Release 12.4(24)T32f.

- CSCtx24021

  The Cisco LTE PGW crashes while sending data traffic when a 4G-to-3G handoff is in progress. This crash is seen only during a race condition when data traffic is being switched during a 4G-to-3G handoff. This condition is rare and exists in Release 1.3.7a and prior releases.

  Workaround: There is currently no known workaround.

- CSCty03897

  Currently, when a PowerPC (PPC) crash due to a BUS error occurs, the PPC does not store the address access that caused the BUS error. This condition occurs when there is a machine check exception.

- CSCty96931

  Cisco PGW might report the DFP weight as zero (0) to the Cisco SLB and get throttled. This happens when the bearer metric value reported by TCOPs on a PGW is 0. This issue is seen only when a very high number of GTPv2 to GTPv1 handoffs are occurring and the sum of current active sessions plus the GTPv2-to-GTPv1 handoff counts exceeds the maximum configured bearer capacity of PGW.

Cisco SAMI Caveats

The following Cisco SAMI caveat is resolved with Cisco LTE PGW Release 1.3.7b, Cisco IOS Release 12.4(24)T32f.

- CSCtx29111

  After a reload, the **show version** command output displays the reload reason as “System returned to ROM by error - Bus Error, PC 0x0.” This condition occurs when a PPC encounters a machine check exception due to a PC bus error.

- CSCtx14679

  The **show version** command output after a Cisco SAMI reload displays the Proxy Control Processor (PCOP) reload reason as “reloaded by admin” when a Traffic and Control Processor (TCOP) reloads because of a machine check exception (PC bus error). This condition exists with a Cisco SAMI reload due to the machine check exception (PC bus error) seen in a TCOP.

- CSCtx23645 (resolved by CSCtx88394)

  Crashinfo and Debuginfo contains only one single line. This condition is not specific to any crash and can occur because of an RF-induced reload, software crash, health monitoring failure, etcetera.

- CSCtx88394

  When a crash (RF-Induced reload/HM-failure) occurs, the “Crashinfo_proc/debuginfo_proc” is missing in the crashinfo_collection.tar file.

Unreproducible Caveats

The following caveats have not been reproduced with Cisco LTE PGW Release 1.3.7b, Cisco IOS Release 12.4(24)T32f.

- CSCtt27485

  A Traffic and Control Plane processor (TCOP) triggers RF-induced reload of the standby.

  This condition occurs due to an “Out of Window” data reception in the TCOP.

- CSCtw60993

  The Cisco SAMI reloads with the following error message:

  ```
  %SAMI-2-SAMI_SYSLOG_CRIT: SAMI 1/0: %SAMI-2-443001: System experienced fatal
  failure.Service name:System Manager (core-server)(30380) has terminated on receiving
  signal 11,reloading system
  ```

  As part of the crash info, the core file “qnx_1_io-net_114693_core” is generated. “114693” is the process ID for network I/O support (io-net), and might vary from case to case.

  Conditions that might cause this reload are not known.

- CSCtx02644

  A few sessions are dropped during a 3G-to-4G handoff.

  This condition occurs when there are a large number of sessions (~10000) for which there is a 3G-to-4G handoff occurring with continuous data transfer. The dropped sessions are not seen with fewer number of sessions (~1000) or when continuous data transfer is not occurring during handoff.

Caveats - Cisco LTE PGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f

This section lists the open, resolved and unreproducible caveats that pertain to Cisco LTE PGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

- Open Caveats, page 34
- Resolved Caveats, page 38

Open Caveats

Note Caveats open in one 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 LTE PGW Caveats, page 34
- Cisco SAMI Caveats, page 37

Cisco LTE PGW Caveats

The following Cisco LTE PGW caveats are open in Cisco IOS Release 12.4(24)T31f.

- CSCtj25287

  During the creation of a session, if a failure response from the IXP occurs while the session is being deleted under a specific timing window (for example, the IXP might already have an entry), the PGW might reload.

  This is a timing condition between the completion of accounting start and the deletion of a session under a specific timing window.

  Workaround: There is currently no known workaround.

- CSCts34338

  The Cisco LTE PGW/SGW might drop an update PDP context requests because of an International Mobile Subscriber Identity (IMSI) mandatory information element (IE) missing error. This condition occurs during a GTPv0-to-GTPv1 handoff or during a GTPv2-to-GTPv1 handoff if the IMSI is not present in the update PDP context request. The PGW/SGW considers this a mandatory IE instead of an optional ID, and drops the incoming request.

  Workaround: There is currently no known workaround.

- CSCts86594

  The counters for the G-PDU bits in the Cisco Mobile Wireless Transport Manger (MWTM) display a negative value.

  Workaround: There is currently no known workaround.

- CSCts90790

  Not all GTPv1 PDPs are cleared on newly active PGW when the restart counter is changed and a failover occurs at the same time.

  Workaround: There is currently no known workaround.

- CSCtt11538

  Incorrect values for APN counters display when a PDP is reassigned to a different Traffic and Control Plane processor (TCOP).

  This condition occurs only when a PDP is reassigned to a different TCOP.

  Workaround: There is currently no known workaround.

- CSCtu10175

  The following syslog message might seen:

  ```
  %IPC-3-SAMI_SM_FAIL_DUP_MSISDN: Unexpected condition: TCOP in IMSI-Sticky doesn't
  match with MSISDN-Sticky.
  ```

  This message might be seen with one of the following:

  a. Inter RAT handoff from UTRAN to E-UTRAN (GTPv1-to-GTPv2 handoff) occurs, if a create session request is received on the SGW without an MSISDN IE, or

  b. TCOP reassignment happens during create-over-create scenario, because the new create request fails on the TCOP where the session exists.

  The message does not appear to impact any functionality.

  Workaround: There is currently no known workaround.

- CSCtu24144

  When polling of cGgsnExtSubscriberTable for GTPv2 calls, the trailing zeros of mobile station ISDNs (MSISDNs) are ignored.

  When there are calls whose MSISDN has trailing zeros, **snmpget** appears to function properly, even if the zeros are omitted, as seen in the following example command output:

```
pgw-03#show gprs gtp pdp-context msisdn
TID               MS Addr      Source  SGW Addr        SGSN Addr       MSISDN              APN
2233445566110010 10.0.3.230   LOCAL   111.111.111.13  N/A             2233445566110000    broadband
```

  Although there is only one session, the following **snmpget** returns same value:

```
snmpget -v 2c 130.130.0.10 -c abc cGgsnExtSubscriberTid.12.50.50.51.51.52.52.53.53.54.54.49.49
CISCO-GGSN-EXT-MIB::cGgsnExtSubscriberTid."223344556611" = STRING: 2233445566110010

snmpget -v 2c 130.130.0.10 -c abc cGgsnExtSubscriberTid.14.50.50.51.51.52.52.53.53.54.54.49.49.48.48
CISCO-GGSN-EXT-MIB::cGgsnExtSubscriberTid."22334455661100" = STRING: 2233445566110010

snmpget -v 2c 130.130.0.10 -c abc
cGgsnExtSubscriberTid.16.50.50.51.51.52.52.53.53.54.54.49.49.48.48.48.48
CISCO-GGSN-EXT-MIB::cGgsnExtSubscriberTid."2233445566110000" = STRING: 2233445566110010
```

  Workaround: Ensure that the scenario like below does not occur (two calls with the same MSISDN, minus two trailing zeros at the end of one):

```
pgw-03#show gprs gtp pdp-context msisdn
TID               MS Addr      Source  SGW Addr        SGSN Addr       MSISDN              APN
2233445566110010 10.0.3.230   LOCAL   111.111.111.13  N/A             2233445566110000    broadband
9933445566113314 10.0.3.250   LOCAL   111.111.111.13  N/A             22334455661100      broadband
```

- CSCtu35882

  Negative values for global and path statistics are retrieved by the Mobile Wireless Transport Manager (MWTM) when polling standby gateway.

  This condition occurs when the MWTM polls the GTP-MIB and the GTPv2-MIB on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCtu41869

  Spurious memory access tracebacks are observed when a GTPv2 session is handed off to a GTPv1 PDP while the session is waiting for an update bearer response. While a traceback is observed, the GTPv2-to-GTPv1 handoff is successful and no impact to functionality is observed.

  This condition occurs only when a GTPv2-to-GTPv1 handoff is occurring while the GTPv2 session is waiting for an update bearer response.

  Workaround: There is currently no known workaround.

- CSCtu51795

  There are no counters present to verify the drops from pending_requestQ per PDP.

  A maximum of 16 PDPs can be queued for processing. Currently, there are no counters to check the current status of the queue, and to see if any messages are dropped from the queue.

  Workaround: There is currently no known workaround.

- CSCtw47142

  The Cisco LTE gateways print the following error message to the console if they receive a Version Not Supported message from the charging gateway.

```
 %GTP-0-CORRUPTED_GTP_BYTE_STREAM: Corrupted byte stream, GSN: 172.16.57.15, Closing
socket
 %GTP-0-PACKETPARSINGERROR: GSN: 172.16.78.83, TID: 00, APN: NULL, Reason: LFN in CHRG
msg should be set
 %GTP-0-PACKETPARSINGERROR: GSN: 172.16.57.15, TID: 00, APN: NULL, Reason: Unexpected
message 0x1A
```

  This condition occurs because the Cisco LTE gateways are unable to parse the Version Not Supported packet. The TCP connection between LTE gateways and the charging gateway is re-established to recover from this condition.

  Workaround: There is currently no known workaround.

- CSCtw50105

  The Cisco Mobile Wireless Transport Manager (MWTM) is unable to scale with the number of entries provided by the GTPv2 MIB path table.

  This condition occurs when GTPv2 reporting is enabled on the MWTM.

  Workaround: Disable GTPv2 reporting on the MWTM.

- CSCtw63171

  The primary charging gateway is active on the Proxy Control Processor (PCOP) and the secondary charging gateway is active on the Traffic and Control Plane processors (TCOPs).

  This condition occurs when the Version Not Support message is received on the gateway PCOP.

  Workaround: The workaround for this condition is present in the code. The PCOP detects the mismatch of charging gateways on different processors and disconnects and reestablishes the TCP connection with the primary charging gateway.

- CSCtx02644

  A few sessions are dropped during a 3G-to-4G handoff.

  This condition occurs when there are a large number of sessions (~10000) for which there is a 3G-to-4G handoff occurring with continuous data transfer. The dropped sessions are not seen with fewer number of sessions (~1000) or when continuous data transfer is not occurring during handoff.

  Workaround: There is currently no known workaround.

- CSCtx24021

  The Cisco LTE PGW crashes while sending data traffic when a 4G-to-3G handoff is in progress.

  This crash is seen only during a race condition when data traffic is being switched during a 4G-to-3G handoff. This condition is rare and exists in Release 1.3.7a and prior releases.

  Workaround: There is currently no known workaround.

Cisco SAMI Caveats

The following Cisco SAMI caveats are open with Cisco IOS Release 12.4(24)T31f.

- CSCtn88798

  In a redundant implementation, one of the Cisco SAMIs remains in a STANDBY-COLD state indefinitely. When in a STANDBY-COLD state, sessions are not sychronized to the standby Cisco SAMI.

  This condition is seen on occasions when both of the Cisco SAMIs that are a part of a redundant implementation are reloaded at very close times.

  Workaround: Reload the Cisco SAMI that is in STANDBY-COLD state.

- CSCts50055

  On rare occasions, a Cisco SAMI coming up as a standby (in a redundant implementation) reloads immediately after booting up because of IXP network processor health monitoring failures.

  These IXP health monitoring failures are only seen on Cisco SAMIs coming up as the standby gateway in a redundant implementation.

  Workaround: The Cisco SAMI reloads correctly on its own on the next attempt.

- CSCtt27485

  A Traffic and Control Plane processor (TCOP) triggers RF-induced reload of the standby.

  This condition occurs due to an “Out of Window” data reception in the TCOP.

  Workaround: There is currently no known workaround.

- CSCtu50827

  The Cisco SAMI reloads due to an LCP-to-PPC health monitoring failure.

  This reload occurs only when the very rare condition of a flash operation happening at the same time a software issues causes a crash.

  Workaround: There is currently no known workaround.

- CSCtu73030

  The Cisco SAMI reboots with following logs displaying at the supervisor console:

  ```
  Card in module slot_num, is being power-cycled off (Module not responding to Keep
  Alive polling)
  ```

  After the reload, the dir core: in LCP does not contain any logs that indicate the reason for the reload.

  It is not clear what conditions trigger this error since there were no specific activities going through the LCP at the time the reload occurred.

  Workaround: There is currently no known workaround.

- CSCtw60993

  The Cisco SAMI reloads with the following error message:

  ```
  %SAMI-2-SAMI_SYSLOG_CRIT: SAMI 1/0: %SAMI-2-443001: System experienced fatal
  failure.Service name:System Manager (core-server)(30380) has terminated on receiving
  signal 11,reloading system
  ```

  As part of the crash info, the core file “qnx_1_io-net_114693_core” is generated. “114693” is the process ID for network I/O support (io-net), and might vary from case to case.

  Conditions that might cause this reload are not known.

  Workaround: There is currently no known workaround.

- CSCtx23645

  Crashinfo and Debuginfo contains only one single line. This condition is not specific to any crash and can occur because of an RF-induced reload, software crash, health monitoring failure, etcetera.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list the caveats that have been resolved with Cisco LTE PGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

Cisco LTE PGW Caveats

The following PGW caveats are resolved with Cisco LTE PGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

- CSCtr74989

  The **show gprs gtp pdp tid** command output might display a “Rcvd byte count” and “Sent byte count” that do not match the “MEF uplink bytes” and “MEF downlink bytes” respectively in the same output. This condition occurs when the P-CDR is closed due to size limit or service record limit or the S-CDR is closed due to size limit or traffic volume container limit.

  CDRs generated subsequently for volume limit might contain less bytes than the configured limit. This condition occurs when the continuous volume trigger is not configured and CDRs are generated for an MS timezone change, followed by volume limit.

- CSCtw88253

  cgprsAccPtActivePdps is not incrementing for GTPv2 sessions. This condition is seen when GTPv2 sessions are created and an SNMP query to cgprsAccPtActivePdps does not return the active PDP count.

- CSCtw90218

  On the Cisco LTE PGW, a memory leak might be observed while PGW processes an Update Bearer Response (UBR) with reject cause from the SGW.

  This memory leak is observed only if the UBR is rejected by the SGW. If the UBR is successful, the memory leak does not occur.

- CSCtx15348

  A memory leak on PGW occurs in the QoS policing structure and in the Packet Filter structure.

  This memory leak occurs with the following:

  a. With a GTPv1-to-GTPv0 session handoff and then the session is deleted as a GTPv0 session, a memory leak of 312 bytes is observed in the QoS policing structure.
  b. When the CRULE is rejected, a memory of 72 bytes is observed in the packet filter structure.

Cisco SAMI Caveats

The following Cisco SAMI caveat is resolved with Cisco LTE PGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

- CSCtu46245

  After certain types of reloads (specified below), the Proxy Control Processor (PCOP) reports the reload reason as “Returned to Rommon due to PC Bus Error 0x0.” The Debuginfo collected for the PCOP as part of the reload is truncated.

  This condition occurs with the following:

  a. A crash initiated by the Traffic and Control Plane processors (TCOPS)
  b. RF-induced reloads initiated by any processor
  c. IXP-to-PPC health monitoring failures

Miscellaneous Caveats

The following miscellaneous caveats are resolved with Cisco LTE PGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

- 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

Unreproducible Caveats

The following PGW caveats have not been reproduced with Cisco LTE PGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

- CSCts08257

  The Cisco SAMI running the Cisco LTE PGW image displays a current balance delete credit that is more than the maximum credit in the **show gprs gtp status** command output.

  The following actions result in this condition:

  a. Create approximately 30,000 GTPv2 sessions.

  b. Delete the sessions in the SGW.

  c. Send continuous downstream data from the PGW to the SGW. The SGW returns an error indication message that initiates the deletion of sessions on the active gateway.

  d. Reload the active gateway such that the standby gateway becomes active.

  e. Wait for the standby to come up and a bulk synchronization occurs.

  f. Reload the active gateway again. The new active gateway still receives the error indication message and PDPs are deleted.

- CSCts14952

  The Cisco SAMI running the Cisco LTE PGW image might end up with stuck sessions after multiple switchovers. This condition occurs when there is a lot of data traffic over 10,000 sessions and then the **clear gprs gtp pdp-context all** command is executed along with multiple switchovers.

- CSCts17810

  After multiple redundancy switchovers, stuck GTPv1 PDPs are observed.

  This condition occurs when the PGW is at full GTPv1 PDP capacity (800,000). After performing multiple switchovers (reloading the active PGW), some stuck sessions are observed on the PGW.

- CSCts57792

  The Cisco SAMI running a Cisco LTE PGW image crashes during an active-to-standby transition when the active gateway is reloaded after the **clear gprs gtp pdp-context all** command has been issued.

  The following actions result in this condition:

  a. Create approximately 60,000 GTPv1 and 60,000 GTPv2 sessions.

  b. Data traffic over 30,000 sessions is continuously sent at any rate.

  c. Issue the **clear gprs gtp pdp-context all** command on the active gateway and afterwards, reload the active gateway.

  At this point, upon a standby-to-active transition, the crash might occur. If it does not, repeating these steps eventually results in a crash.

- CSCtu74967

  During a standby to active state transition, the following message is seen:

  ```
  %PLATFORM-3-UNFORESEEN: Free PDP already sent for index
  ```

  This message is seen only when the standby gateway transitions to active while PDPs in the currently active gateway are in deleting state.

Caveats - Cisco LTE PGW Release 1.3.7, Cisco IOS Release 12.4(24)T3f

This section lists the open, resolved and unreproducible caveats that pertain to Cisco LTE PGW Release 1.3.7, Cisco IOS Release 12.4(24)T3f.

Open Caveats

Note Caveats open in one 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 LTE PGW Caveats

The following Cisco LTE PGW caveats are open in Cisco IOS Release 12.4(24)T3f.

- CSCtj25287

  During the creation of a session, if a failure response from the IXP occurs while the session is being deleted under a specific timing window (for example, the IXP might already have an entry), the PGW might reload.

  This is a timing condition between the completion of accounting start and the deletion of a session under a specific timing window.

  Workaround: There is currently no known workaround.

- CSCts08257

  The Cisco SAMI running the Cisco LTE PGW image displays a current balance delete credit that is more than the maximum credit in the **show gprs gtp status** command output.

  The following actions result in this condition:

  a. Create approximately 30,000 GTPv2 sessions.
  b. Delete the sessions in the SGW.
  c. Send continuous downstream data from the PGW to the SGW. The SGW returns an error indication message that initiates the deletion of sessions on the active gateway.
  d. Reload the active gateway such that the standby gateway becomes active.
  e. Wait for the standby to come up and a bulk synchronization occurs.
  f. Reload the active gateway again. The new active gateway still receives the error indication message and PDPs are deleted.

  Workaround: There is currently no known workaround.

- CSCts14952

  The Cisco SAMI running the Cisco LTE PGW image might end up with stuck sessions after multiple switchovers. This condition occurs when there is a lot of data traffic over 10,000 sessions and then the **clear gprs gtp pdp-context all** command is executed along with multiple switchovers.

  Workaround: There is currently no known workaround.

- CSCts34338

  The Cisco LTE PGW/SGW might drop an update PDP context requests because of an International Mobile Subscriber Identity (IMSI) mandatory information element (IE) missing error. This condition occurs during a GTPv0-to-GTPv1 handoff or during a GTPv2-to-GTPv1 handoff if the IMSI is not present in the update PDP context request. The SGW considers this a mandatory IE instead of an optional ID, and drops the incoming request.

  Workaround: There is currently no known workaround.

- CSCts57792

  The Cisco SAMI running a Cisco LTE PGW image crashes during an active-to-standby transition when the active gateway is reloaded after the **clear gprs gtp pdp-context all** command has been issued.

  The following actions result in this condition:

  a. Create approximately 60,000 GTPv1 and 60,000 GTPv2 sessions.
  b. Data traffic over 30,000 sessions is continuously sent at any rate.
  c. Issue the **clear gprs gtp pdp-context all** command on the active gateway and afterwards, reload the active gateway.

  At this point, upon a standby-to-active transition, the crash might occur. If it does not, repeating these steps eventually results in a crash.

  Workaround: There is currently no known workaround.

- CSCts86594

  The counters for the G-PDU bits in the Cisco Mobile Wireless Transport Manger (MWTM) display a negative value.

  Workaround: There is currently no known workaround.

- CSCts90790

  Not all GTPv1 PDPs are cleared on newly active PGW when the restart counter is changed and a failover occurs at the same time.

  Workaround: There is currently no known workaround.

- CSCtt11538

  Incorrect values for APN counters display when a PDP is reassigned to a different Traffic and Control Plane processor (TCOP). This condition occurs only when a PDP is reassigned to a different TCOP.

  Workaround: There is currently no known workaround.

- CSCtu10175

  The following syslog message might seen:

  ```
  %IPC-3-SAMI_SM_FAIL_DUP_MSISDN: Unexpected condition: TCOP in IMSI-Sticky doesn't
  match with MSISDN-Sticky.
  ```

  This message might be seen with one of the following:

  a. Inter RAT handoff from UTRAN to E-UTRAN (GTPv1-to-GTPv2 handoff) occurs, if a create session request is received on the SGW without an MSISDN IE, or

  b. TCOP reassignment happens during create-over-create scenario, because the new create request fails on the TCOP where the session exists.

  The message does not appear to impact any functionality.

  Workaround: There is currently no known workaround.

- CSCtu21137

  RF-induced reloads are triggered by the Traffic and Control Plane processors (TCOPs). This condition occurs in an Active/Standby redundant implementation.

  Workaround: There is currently no known workaround.

Cisco SAMI Caveats

The following Cisco SAMI caveats are open with Cisco IOS Release 12.4(24)T3f.

- CSCtn88798

  In a redundant implementation, one of the Cisco SAMIs remains in a STANDBY-COLD state indefinitely. When in a STANDBY-COLD state, sessions are not sychronized to the standby Cisco SAMI.

  This condition is seen on occasions when both of the Cisco SAMIs that are a part of a redundant implementation are reloaded at very close times.

  Workaround: Reload the Cisco SAMI that is in STANDBY-COLD state.

- CSCts50055

  On rare occasions, a Cisco SAMI coming up as a standby (in a redundant implementation) reloads immediately after booting up because of IXP network processor health monitoring failures.

  These IXP health monitoring failures are only seen on Cisco SAMIs coming up as the standby gateway in a redundant implementation.

  Workaround: Reload the Cisco SAMI. The module usually reloads correctly on the next attempt.

- CSCts50077

  The Cisco SAMI reloads because of a health monitoring failure and the following syslog message is generated:

  ```
  %PLATFORM-4-DP_HM_WARN: Failed to receive response from IXP1 in 22 retries, system
  will reboot if it continues to fail receiving response in another 8 retries (i.e. in
  the next 80 secs.) Check `sami health-monitoring' configuration and see `show sami
  health-monitoring' for more info
  ```

  This condition occurs when the Cisco SAMI network processor (IXP) fails to respond to health monitor messages sent from a PowerPC (PPC).

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list the caveats that have been resolved with Cisco LTE PGW Release 1.3.7, Cisco IOS Release 12.4(24)T3f.

- Cisco LTE PGW Caveats, page 45
- Cisco SAMI Caveats, page 47

Cisco LTE PGW Caveats

This section lists the PGW caveats that are resolved with Cisco LTE PGW Release 1.3.7, Cisco IOS Release 12.4(24)T3f.

- 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.

- CSCtq70842

  When an **snmpwalk** is run on a complete Management Information Base (MIB) Object Identifier (OID) tree against an SGW or PGW that has no bearers/PDPs, the CPU usage is approximately 20 percent. With 50,000 create and delete session requests, but no **snmpwalk** running, the CPU usage is approximately 20 percent. However, when an **snmpwalk** and the 50,000 create and delete session requests are combined, the CPU usage climbs to 99 percent.

  The high CPU condition is seen when the 50,000 create and delete session requests and an **snmpwalk** of the entire MIB tree occur at the same time.

- CSCtr30404

  The SNMP-ENGINE process might leak memory on the PGW/SGW gateways when the path history table is polled.

- CSCts63514

  GTP Version 1 (GTPv1) PDPs become stuck during standby-to-active switchover.

  This condition occurs with the Cisco LTE SGW or Cisco LTE PGW when PDPs are being deleted because of a new recovery information element (IE) value in the active gateway, which indicates a path restart, while the standby gateway is coming up and starts receiving bulk synchronization for create PDPs from the active gateway.

  The active gateway immediately reloads after the bulk synchronization when there are PDPs remaining on the restarting path of the active gateway.

- CSCts69614

  A high CPU is seen on the PGW when the maximum CPU is taken by the SNMP engine single IP stats A process.

  This condition is seen on the PGW when the PGW had 1600 GTP paths and the Cisco Mobile Wireless Transport Manager (MWTM) polls the following SNMP tables:

  – CISCO-GTP-MIB

    - cGtpPathTable

    - cGtpPathStatisticsTable

  – CISCO-GTPV2-MIB

    - cGtpPathGtpv2StatisticsTable

    - cGtpPathGtpv2ReqMsgTable

    - cGtpPathGtpv2RspMsgTable

- CSCts85619

  The Cisco Mobile Wireless Transport Manager (MWTM) has negative values for PDP activation statistics

  This condition is seen when the MWTM polls the standby PGW for the following objects:

  – cgprsAccPtTotRmtInitCreateBearers

  – cgprsAccPtSuccRmtInitCreateBearers

- CSCtt07560

  In a redundant implementation, the following traceback appears on the active gateway 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 gateway state is “ACTIVE,” the traceback stops displaying.

- CSCtt71202

  A high CPU is seen on the Cisco LTE gateway (PGW or SGW) with an SNMP GetBulk request on an object identifier (OID) polls the subscriber table.

- CSCtu27352

  The gateway crashes when displaying path history tables. The path history tables are not empty and entries change simultaneously when the **show gprs gtp path history** command is executed.

Cisco SAMI Caveats

The following Cisco SAMI caveats are resolved with Cisco LTE PGW Release 1.3.7, Cisco IOS Release 12.4(24)T3f.

- 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.

- 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.

- CSCts73976

  When the Cisco SAMI IXP statistics counters increase to larger values, writing those values to print buffer causes the following traceback:

  ```
  SAMI 2/3: 000049: Sep 17 22:08:58: %SAMI-4-WARNING: Unexpected condition: Bad
  string length, output truncated -Process= "Virtual Exec", ipl= 0, pid= 243,  -
  Traceback= 0x4586BB38z 0x4586BC28z 0x4586F7B8z 0x448A9B0Cz 0x44888930z
  0x4585E9ACz 0x44888A98z 0x448A9B0Cz 0x448D06F0z 0x459906F8z
  0x45993DFCzATTSGW52#
  ```

  This traceback is visible when the **show tech** command or **show sami ixp statistics** command is executed. Additionally, this traceback causes no functional impact and is more likely to occur if the Cisco SAMI has been up for multiple days.

- CSCts85619

  Cisco Mobile Wireless Transport Manager (MWTM) displays negative values for PDP activation statistics when the MWTM polls the standby node for the “cgprsAccPtTotRmtInitCreateBearers” and “cgprsAccPtSuccRmtInitCreateBearers” objects.

- CSCtt32257

  While debugging, it is observed on rare occasions that all of the lookup threads become stuck, resulting in the IXP not processing any packets. The Cisco SAMI IXP has more than 50 look threads. If a few threads fail, the system might not report the failure right away, but continue to work in degraded mode.

- CSCtt37393

  Scheduled jobs (cron table jobs) execute the **write memory** command on the Cisco SAMI Traffic and Control Plane processors (TCOPs). The cron job is a distributed command, which means it is propagated to the TCOPs.

  The Cisco SAMI single IP architecture does not use TCOP configuration files in NVRAM. The TCOP configurations are driven by the PCOP, which retrieves the configuration file from the supervisor. Executing the **write memory** command in the TCOPs saves the configuration in the TCOP NVRAM. This is an unnecessary and redundant write to NVRAM.

  With this fix, the **write memory** command is disabled at the TCOPs.

Caveats - Cisco LTE PGW Release 1.3.6, Cisco IOS Release 12.4(24)T3e

This section lists the open, resolved and unreproducible caveats that pertain to Cisco LTE PGW Release 1.3.6, Cisco IOS Release 12.4(24)T3e.

- Open Caveats, page 48
- Resolved Caveats, page 45

Open Caveats

Note Caveats open in one 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 LTE PGW Caveats, page 48
- Cisco SAMI Caveats, page 50

Cisco LTE PGW Caveats

The following Cisco LTE PGW caveats are open in Cisco IOS Release 12.4(24)T3e.

- CSCtq70842

  When an **snmpwalk** is run on a complete Management Information Base (MIB) Object Identifier (OID) tree against an SGW or PGW that has no bearers/PDPs, the CPU usage is approximately 20 percent. With 50,000 create and delete session requests, but no **snmpwalk** running, the CPU usage is approximately 20 percent. However, when an **snmpwalk** and the 50,000 create and delete session requests are combined, the CPU usage climbs to 99 percent.

  The high CPU condition is seen when the 50,000 create and delete session requests and an **snmpwalk** of the entire MIB tree occur at the same time.

  Workaround: There is currently no known work around.

- CSCts50077

  The Cisco SAMI reloads because of a health monitoring failure and the following syslog message is generated:

  ```
  %PLATFORM-4-DP_HM_WARN: Failed to receive response from IXP1 in 22 retries, system
  will reboot if it continues to fail receiving response in another 8 retries (i.e. in
  the next 80 secs.) Check `sami health-monitoring' configuration and see `show sami
  health-monitoring' for more info
  ```

  This condition occurs when the Cisco SAMI network processor (IXP) fails to respond to health monitor messages sent from a PowerPC (PPC).

  Workaround: There is currently no known workaround.

- CSCts63514

  GTP Version 1 (GTPv1) PDPs become stuck during standby-to-active switchover.

  This condition occurs with the Cisco LTE SGW or Cisco LTE PGW when PDPs are being deleted because of a new recovery information element (IE) value in the active gateway, which indicates a path restart, while the standby gateway is coming up and starts receiving bulk synchronization for create PDPs from the active gateway.

  The active gateway immediately reloads after the bulk synchronization when there are PDPs remaining on the restarting path of the active gateway.

  Workaround: There is currently no known workaround.

- CSCts69614

  A high CPU is seen on the PGW when the maximum CPU is taken by the SNMP engine single IP stats A process.

  This condition is seen on the PGW when the PGW had 1600 GTP paths and the Cisco Mobile Wireless Transport Manager (MWTM) polls the following SNMP tables:

  – CISCO-GTP-MIB

    - cGtpPathTable

    - cGtpPathStatisticsTable

  – CISCO-GTPV2-MIB

    - cGtpPathGtpv2StatisticsTable

    - cGtpPathGtpv2ReqMsgTable

    - cGtpPathGtpv2RspMsgTable

  Workaround: Use the following configuration to block the SNMP object identifiers (OIDs) so that they are not available for SNMP polling:

  – **snmp-server view SMI iso included**

  – **snmp-server view SMI cGtpPathTable excluded**

  – **snmp-server view SMI cGtpPathStatisticsTable excluded**

  – **snmp-server view SMI cGtpPathStatisticsTable excluded**

  – **snmp-server view SMI cGtpPathGtpv2StatisticsTable excluded**

  – **snmp-server view SMI cGtpPathGtpv2ReqMsgTable excluded**

  – **snmp-server view SMI cGtpPathGtpv2RspMsgTable excluded**

  – **snmp-server community** *removed* **view SMI** *RO/RW*

- CSCts85619

  Cisco Mobile Wireless Transport Manager (MWTM) displays negative values for PDP activation statistics when the MWTM polls the standby node for the “cgprsAccPtTotRmtInitCreateBearers” and “cgprsAccPtSuccRmtInitCreateBearers” objects.

  Workaround: Configure MWTM to use the Hot Standby Router Protocol (HSRP) IP address to poll the gateways instead of the physical interface addresses of individual gateways.

- CSCts86594

  The counters for the G-PDU bits in the Cisco Mobile Wireless Transport Manger (MWTM) display a negative value.

  Workaround: There is currently no known workaround.

Cisco SAMI Caveats

There are no known Cisco SAMI caveats open with Cisco IOS Release 12.4(24)T3e.

Resolved Caveats

The following sections list the caveats that have been resolved with Cisco LTE PGW Release 1.3.6, Cisco IOS Release 12.4(24)T3e.

- Cisco LTE PGW Caveats, page 50
- Cisco SAMI Caveats, page 53

Cisco LTE PGW Caveats

This section lists the PGW caveats that are resolved with Cisco LTE PGW Release 1.3.6, Cisco IOS Release 12.4(24)T3e.

- CSCtq74610

  The Cisco LTE PGW crashes when handling a RADIUS Change of Authorization (CoA) message from the Cisco CSG2 under stress conditions with a slow Policy and Charging Rules Function (PCRF).

  This issue occurs under the following conditions:

  - 200 calls per second creating 60K sessions.
  - Within 60 seconds of a CSR, an MBR is sent.
  - A slow PCRF results in several authentication/accounting failures.

- CSCtq93374

  The QoS class identifier (QCI) and allocation retention priority (ARP) values in the SGW and PGW are out of sync.

  This condition exists when a GTPv2 create request with a Policy and Charging Rules Function (PCRF) responding with a different set of QoS than the User Equipment requested QoS.

- CSCtr03444

  The PGW crashes during a GTPv0 create when a GTPv0 PDP exists with the same tunnel ID (TID) under a different access-point (APN).

  This condition is seen only when there is an APN-related failure while creating a GTPv0 PDP. The list of such failures are as follows:

  - When a create request comes with a TID that already exists under a different APN.
  - The APN is not configured.
  - The type of APN selected is virtual.
  - The APN configuration does not match the type of PDP context.
  - If APN subscription is required but not verified.

- CSCtr14267

  The following error messages might appear on the PGW:

  ```
  SAMI 6/5: 000105: Jun 21 06:53:27: %GPRSFLTMG-4-CHARGING: GSN: , TID:
  0000000000000000, APN: NULL, Reason: 0, unexpected CSG usage report cause -Traceback=
  0x443D37E8z 0x4435C498z 0x4435C7FCz 0x4435D40Cz 0x44352010z 0x44352EC8z 0x4435327Cz
  0x4598BB78z 0x4598F27Cz
  ```

  This condition occurs whenever a PGW-initiated QoS update request fails as is indicated by the appearance of the following syslog message.

  ```
  SAMI 6/4: 000182: Jun 22 10:06:48: %GPRSFLTMG-4-GTPv1_PDP_UPDATE_FAIL: GSN:
  135.211.131.2, TEID: 232189D, APN: testbroadbandvtccz3, Reason: 1, SGSN does not
  support GGSN initiated PDP QOS update
  ```

  When charging is enabled and the PGW is generating P-CDRs, this condition will also occur as the result of the addition of service containers to the ListOfServiceData with a serviceChangeCondition value of “0”.

- CSCtr15095

  Cisco CSG2 link flapping is seen because out of sequence messages from the CSG2 are received. The flap is observed when a PGW failover occurs and an out of user sequence service control usage (SCU) message is received.

  The condition occurs in a Gx topology (PGW+CSG2+Policy and Charging Rules Function [PCRF]) when a PGW failover occurs, the Cisco CSG2 sends out of user sequence SCU message to the PGW, and the PGW does not acknowledge that it has received the SCU.

- CSCtr20034

  The Cisco PGW quota server interface sends a GTP reject cause code to the Cisco CSG2 for several conditions where the PGW decides to discard service usage, for example, with retransmitted usage when the received usage is outside the expected sequence window or the user is not found.

  With this fix, the PGW sends the reject cause code for the usage only when the actual sanity of the service control message fails (for example, with parse error codes). Otherwise, the PGW sends an acknowledgement to the service control message because there is no defect with the message.

  With this fix, a **detailed** keyword option has been added to the **show ggsn csg statistics** command (**show ggsn csg statistics** [**detailed**]), which enables you to display enhanced statistics for the service control message processing on the quota server interface.

- CSCtr25021

  A stale PDP is seen on the standby PGW when the bearer/PDP is sychronized to the standby while it is in a deleting state.

- CSCtr25880

  The number of service records buffered counter does not decrement.

  This condition occurs when there is no call detail record (CDR) opened for the service record buffered.

- CSCtr29258

  When path table cGtpPathGtpv2ReqMsgTable or cGtpPathGtpv2RspMsgTable is polled frequently while PDP contexts are being created and deleted on the PGW, sometimes SNMP lexicographical ordering breaks and an Index with a much lesser value leading to an SNMP loop is received.

  The issues occurs under the following conditions:

  a. The PGW is processing multiple create and delete PDP requests from different SGSNs.
  b. The cGtpPathGtpv2ReqMsgTable and cGtpPathGtpv2RspMsgTable MIB table is polled frequently.

- CSCtr30296

  The PGW crashes when a 3G-to-4G handoff occurs when a 3G procedure that has been initiated by the PGW is pending, and is followed by a 4G session delete or failure.

- CSCtr30916

  A high CPU occurs during the creation of a GTPv0 PDP over an existing GTPv1 PDP.

  The high CPU is seen only when an existing GTPv1 PDP is waiting for an update to be completed and a GTPv0 create request is initiated.

  The fix for the particular symptom is in CSCtr31369. Additionally, the fix committed with CSCtr30916 resolves this condition by freeing the CPU by dropping the new create request.

- CSCtr31369

  High CPU occurs during the creation of GTPv0 PDPs over existing GTPv1 PDPs.

  This condition is seen only when the existing GTPv1 PDP is waiting for an update to be completed and a GTPv0 create request is initiated.

- CSCtr70157

  Lawful interception fails to do provision a mediation device (MD) and an **snmpset request** returns a “No-Creation” error. Additionally, an **snmpwalk** returns nothing from the SNMP Mediation Table.

  This condition occurs only when the incorrect ifIndex is used in **snmpset**.

- CSCtr91619

  The%GPRSFLTMG-6-GPRS_CHARGING_NO_CDR message displays on the newly active PGW after a switchover.

  This message might be seen during a standby to active PGW switchover when there are active subscriber sessions with service-awareness enabled.

- CSCtr93869

  For unknown reasons, the Cisco LTE PGW displays “NO_CDR” syslog when a CDR closes.

  This condition occurs on the active PGW.

- CSCts46701

  A CPU usage spike of more than 90 percent occurs when polling cIpLocalPoolAllocTable objects.

  This condition occurs when polling the cIpLocalPoolAllocTable or an **snmp getbulk** is executed against the ciscoIpLocalPoolMIB, which can internally poll cIpLocalPoolAllocTable objects.

- CSCts49152

  Cisco LTE PGW crashes during a PDP cleanup.

  This condition occurs when:

  a. Per PDP policing is enabled and configured under an APN.

  b. A GTPv1 to GTPv0 handoff occurs for a PDP for which QoS policing is enabled and the PDP is the last PDP associated with a specific rate profile.

  c. The PDP is either deleted or a handoff back to GTPv1 PDP occurs.

Cisco SAMI Caveats

This section lists the Cisco SAMI caveats that are resolved with Cisco LTE PGW Release 1.3.6, Cisco IOS Release 12.4(24)T3e.

- CSCtq88202

  The **ucdump -t** command does not recognize VLAN and L2VD tables as valid arguments.

  This condition only relates to the display of the VLAN and L2VD tables using the **ucdump -t** command from the IXP console. The tables are setup correctly and traffic is forwarded successfully based on these tables.

- CSCtr31428

  The Cisco SAMI IXP micro-engine threads used to configure data paths might take a lock on tables and not freeing it, thereby holding the lock indefinitely.

  This fix catches these issues for debugging purposes. Use the **ucdump -t LOCK** command to dump debugging information when a lock is held infinitely.

- CSCtr31558

  Continuous IXP IPC failure error messages are seen from the Cisco SAMI:

  ```
  %PLATFORM-3-SAMI_IPC_IXP_FAIL: IPC timed out for IXP<ixp no> for Msgcode <msg>, Num
  tries: <tries>
  ```

  This condition typically occurs when the Cisco SAMI IXP stops processing IPC messages from the Cisco SAMI processors.

- CSCtr32854

  The syslog messages “PLATFORM-3-SAMI_IPC_IXP_FAIL:” is observed when the Cisco SAMI IXP receives out of order configuration messages, for example, when the IXP receives a modify PDP request before a create PDP request or after a free PDP message.

- CSCtr81828

  The Cisco SAMI reloads with the following syslog error message

  ```
  "%PLATFORM-1-DP_HM_FAIL: Failed to receive response from IXP<1/2>. Check 'sami
  health-monitoring' configuration and see 'show sami health-monitoring' for more info"
  ```

  The condition occurs when the network processor (IXP) fails to respond to Health Monitoring (HM) messages sent by the SAMI PowerPCs (PPCs).

  The IXP maintains packets, including HM messages, in DRAM buffers. The pointers to these buffers (also known as the buffer handles) are maintained by q-arrays. Expected behavior is that the q-arrays provide valid buffer handles, however, when a Null (invalid) buffer handle is de-queued by q-array, the hardware assist, which maintains the q-array buffer becomes corrupted and the IXP reaches a state where it does not process incoming packets any longer.

Caveats - Cisco LTE PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c

This section lists the open, resolved and unreproducible caveats that pertain to Cisco LTE PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

- Open Caveats, page 54
- Resolved Caveats, page 55
- Unreproducible Caveats, page 59

Open Caveats

Note Caveats open in one 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 LTE PGW Caveats, page 60
- Cisco SAMI Caveats, page 61

Cisco LTE PGW Caveats

This section lists the PGW caveats that are open with Cisco LTE PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

- CSCtq74610

  The Cisco LTE PGW crashes when handling a RADIUS Change of Authorization (CoA) message from the Cisco CSG2 under stress conditions with a slow Policy and Charging Rules Function (PCRF).

  This issue occurs under the following conditions:

  - 200 calls per second creating 60K sessions.
  - Within 60 seconds of a CSR, an MBR is sent.
  - A slow PCRF results in several authentication/accounting failures.

  Workaround: There is currently no known workaround.

- CSCtq82202

  In a redundant implementation, the standby PGW undergoes a self-induced reload when there is a lot of synchronization activity from the active PGW that was triggered by the creation of sessions due to create session requests and the deletion of sessions due to failure of either the bearer resource command (BRC) or the modify bearer command (MBC) procedures.

  This condition occurs only when there are a high number of failures resulting from either BRC or MBC procedures.

  Workaround: There is currently no known workaround.

Cisco SAMI Caveats

This section lists the SAMI caveats that are open with Cisco LTE PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

- CSCti31555

  For dual stack sessions belonging to APNs with Mobile Express Forwarding (MEF) switching enabled, the "MEF uplink packets / links" field displays some non zero values immediately after the sessions come up.

  This condition occurs when sessions belonging to an APN, which has dual stack configured (using the **gtp bearer dual-addr** access-point configuration command) and has MEF switching enabled. The **show gprs gtp pdp-context tid** command output displays some non zero values in the "MEF uplink packets / links" field.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list the caveats that have been resolved with Cisco LTE PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

- Cisco LTE PGW Caveats, page 61
- Cisco SAMI Caveats, page 62
- Miscellaneous Caveats, page 59

Cisco LTE PGW Caveats

This section lists the PGW caveats that are resolved with Cisco LTE PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

- CSCtj11112

  In a redundant implementation, the Cisco LTE PGW rejects a RADIUS Change of Authorization (CoA) because of an existing CoA outstanding error message on newly active PGW after switchover.

  This condition is seen for existing sessions on the newly active PGW after a switchover with Cisco LTE PGW releases prior to Release 1.3.5.

- CSCtj43523

  The pre Release 8 Quality of Service (QoS) status counters are not incremented in the output of the **show gprs qos status** privileged EXEC command.

  This condition occurs when a GTPv1 PDP context is created on a UMTS QoS class.

- CSCtj99979

  The Cisco LTE PGW does not delete PDP contexts after an idle PDP context timeout occurs.

  This condition occurs when the session idle timeout is configured and a GTPv0 PDP is created and left idle. When the timeout occurs, the PDP is not deleted.

- CSCtk83766

  When the **limit volume** *yyy* command is configured under a charging profile, the **limit volume** *yyy* **reset** command does not work, and vice versa.

  This condition occurs when the values for the two commands are not the same.

- CSCto03189 3

  When a BSM Resource Controller (BRC) is sent to the Cisco LTE PGW to replace the existing uplink (UL) and downlink (DL) install filters, the PGW replaces the UL filter, but it adds the filter received from the Policy Control and Charging Rules Function (PCRF) on the DL instead of replacing it.

  This condition occurs when a Policy and Charging Control (PCC) session is created using the default settings and a BRC is sent to the PGW to replace existing filters.

- CSCtq15406

  Spurious memory access is seen on the Cisco LTE PGW when a GTPv2 session is created over GTPv0 because incorrect data structure is being accessed.

- CSCtq17144

  In a redundant implementation, the standby gateway has some stale sessions but the active gateway has none. The standby sessions should be in a “deleting” state.

- CSCtq17447

  On the Cisco LTE PGW a traceback occurs with the following message:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_don while session deletion
  ```

- CSCtq17797

  In a redundant implementation, a new standby gateway crashes during bulk sychronization.

  This condition occurs when Quality of Service (QoS) profile on the Policy and Charging Rules Function (PCRF) is configured to initiate dedicated bearers.

- CSCtq18845

  The Cisco LTE PGW reloads.

  This condition occurs after hours of 4G traffic running at high create/delete sessions per second rate (approximately 500 create/deletes per second) and a continuous fail/re-enable Policy and Charging Rules Function (PCRF).

- CSCtq23278

  The Cisco LTE PGW sends the incorrect SGSN address in the service container after an SGW handover.

  This condition is seen when both the Cisco LTE SGW and a public land mobile network (PLMN) change occurs.

- CSCtq42803

  When a GTPv1 to GTPv2 handoff request is received for a GTPv1 PDP that is in the process of being deleted and waiting on the final SCU, the Cisco LTE PGW might crash.

  This condition is seen under the following circumstances:

  1. The path to the Cisco CSG2 is down.
  2. The peer is restarted.
  3. A GTPv1 to GTPv2 request is received for an existing PDP context.

- CSCtq44823

  In a redundant implementation, the active gateway does not synchronize Quality of Service (QoS) values that are received from the Policy and Charging Rules Function (PCRF) during negotiation to the standby gateway. This causes inconsistent redundant setups for QoS values and the standby will apply the default QoS values on the subscriber traffic after a switchover occurs.

  This condition is seen on the standby gateway in a redundant implementation when the active gateway receives QoS values from PCRF during negotiation.

- CSCtq45087

  In a redundant implementation, the active gateway does not synchronize Maximum Bit Rate (MBR)/Guaranteed Bit Rate (GBR) uplink/downlink values negotiated by Policy and Charging Rules Function (PCRF) to the standby gateway. Therefore, the values are not reflected on the standby gateway.

  This condition occurs on the standby gateway in a redundant implementation when the active gateway receives Quality of Service (QoS) values from PCRF.

- CSCtq52753

  When the default (empty) policy-profile is applied to an APN, the Cisco LTE PGW applies the Aggregate Maximum Bit Rate (AMBR) values to a GTPv1 session after a GTPv2 to GTPv1 handover occurs. Use the **show gprs gtp pdp-context tid** *tid* **qos police** privileged EXEC command to display the values applied to the session.

  This condition occurs when policing is configure on an APN.

- CSCtq54836

  When a Tracking Area Identifier (TAI) change occurs from a User Location Information (ULI) type other than TAI or Routing Area Identifier (RAI), call detail records (CDRs) are closed with a public land mobile network (PLMN) ID change as the cause.

  This condition occurs when the PGW receives a create session request with an ULI type other than TAI/RAI, and then receives a modify bearer request or delete session request with TAI/RAI.

- CSCtq55745

  After an enhanced quota server interface is unconfigured by using the **ggsn quota-server** *server-name* **service-msg** global configuration command, PDP contexts become stuck in a "deleting" state after issuing the **clear gprs gtp pdp all** privileged EXEC command.

  This condition occurs when service-aware sessions exist, the enhanced quota server interface is unconfigured, and then the **clear gprs gtp pdp context** command is issued. Instead of being deleted, the service-aware PDP contexts become stuck in a deleting state.

- CSCtq57150

  In a redundant implementation, when the Cisco CSG2 path is down, stuck sessions are seen on the active PGW when the peer restarts and sends a new create request for an existing session.

  This condition occurs only when the Cisco CSG2 path is down, there is an existing GTPv1 PDP context, and then the peer restarts and sends a new create request for the existing PDP.

- CSCtq58699

  GTPv1 PDP contexts remained stuck and are not deleted even after attempting to manually clear them when the path between the Cisco LTE PGW and Cisco CSG2 is flapping and Service Control Requests (SCRs) are being sent at a rate high enough to cause more than 12500 outstanding SCRs per Traffic and Control Plane processor (TCOP).

  This condition occurs only when SCRs are timing out because the path between the PGW and CSG2 is flapping and a large number of pending SCRs exist in the system (more than 12500 SCRs per TCOP).

- CSCtq60091

  In a redundant implementation, PDP contexts are deleted after two switchovers occur.

  This condition can be seen when a GTPv1 PDP is created, the active gateway reloads, a handoff from GTPv1 to GTPv2 occurs, and the active gateway reloads once again. The PDP context is not created on the standby gateway, but the PDP context exists on the active gateway.

- CSCtq63301

  In a redundant implementation, a traceback occurs on the active PGW during a switchover.

  This condition occurs when a redundancy state changes when a GTPv2 PDP is in a half-created state.

- CSCtq63866

  The **show gprs charging profile** command displays an incorrect value for the Continue Option for Volume Limit trigger. The value displays as Enabled when it is Disabled, and vice versa.

  The continuity trigger for duration should be enabled if continuity trigger for volume is disabled and the continuity trigger for duration should be disabled if continuity trigger for volume is enabled.

- CSCtq67546

  In a redundant implementation, when a standby to active switchover occurs when there are existing PDP contexts waiting on the final SCU to be received from the Cisco CSG2, the final usage might be lost.

  This condition occurs when the newly active PGW does not wait on the SCU and deletes the PDP contexts as soon as the its redundancy state changes to active. This issue is seen only when PGW switchover occurs and there are PDPs contexts waiting for final SCU from the Cisco CSG2.

- CSCtq71043

  On the Cisco LTE PGW, the following syslog message might appear:

  ```
  Syslog %GPRSFLTMG-3-GPRS_CHARGING_NO_CDR: No Open CDR
  ```

  This condition occurs when the quota server interface on the PGW is overloaded, or in any other situation where "Out of Order Usage Messages" (SCUs) are received by the PGW.

  The usage reporting reason is falsely interpreted on the PGW. If the usage report reason is interpreted as PDP closure, the existing CDR might be closed, and all subsequent usage for the PDP context might not be reported and the syslog message appears.

Cisco SAMI Caveats

This section lists the Cisco SAMI caveats that are resolved with Cisco LTE PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

- CSCtk12410

  When two Cisco SAMIs are configured as an active standby pairs, 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.

- CSCto98454

  Upstream data packets are dropped in the Cisco SAMI IXP network processor path. Issuing the **show gprs gtp pdp-context tid** *tid* privileged EXEC command displays the number of Mobile Express Forwarding (MEF) dropped packets incrementing.

  This condition occurs when the L2/MAC address to redirect address (Cisco CSG2) is not resolved.

Miscellaneous Caveats

This section lists a miscellaneous Cisco IOS software caveat that is resolved with Cisco LTE PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

- CSCtc68037

  A Cisco IOS device might experience an unexpected reload as a result of mtrace packet processing

Unreproducible Caveats

This section lists caveats that are unreproducible in Cisco LTE PGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

- CSCtq63118

  After a system reload, both gateways in a redundant implementation might end up in an active or active-drain state. This condition is rarely seen, and only occurs when both gateways in a redundant implementation are reloaded at almost the same time. This condition is more likely to occur when the Stream Control Transmission Protocol (SCTP) connectivity for the redundant configuration is lost.

- CSCtq54934

  An SNMP getmany request triggered on ciscoGprsAccPtMIB from an SNMP manager on the gateway times out without receiving a response for a objects in ciscoGprsAccPtMIB.

  This condition occurs when the SNMP getmany request is continuously triggered (in a loop) on the ciscoGprsAccPtMIB.

- CSCtq74652

  When Remote Console and Logging (RCAL) is enabled on the Cisco SAMI, the RCAL **show proc cpu** and the **show proc memory** commands cause the Traffic and Control Plane processor (TCOP) CPU to become stuck at 99% usage.

  This CPU issue is observed after a few hours of experiencing the following conditions:

  a. 66K sessions are created and deleted at 300 calls per sec.
  b. Standby gateway is continuously reloading.
  c. The charging gateway interface is flapping.
  d. A script is executed every 5 seconds that executes the following commands

     show proc cpu | include five seconds

     show gprs gtp status | inc activated session

     show gprs gtp status | inc activated sessions

     show proc mem | include Processor

     show proc mem | include I/O

Caveats - Cisco LTE PGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d

This section contains open and resolved caveats that pertain to Cisco LTE PGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d.

Open Caveats

Note Caveats open in one 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 LTE PGW Caveats, page 60
- Cisco SAMI Caveats, page 61

Cisco LTE PGW Caveats

There are no known PGW caveats open in Cisco LTE PGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d.

Cisco SAMI Caveats

This section lists the SAMI caveats that are open with Cisco LTE PGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d.

- CSCti31555

  For dual stack sessions belonging to APNs with Mobile Express Forwarding (MEF) switching enabled, the "MEF uplink packets / links" field displays some non zero values immediately after the sessions come up.

  This condition occurs when sessions belonging to an APN, which has dual stack configured (using the **gtp bearer dual-addr** access-point configuration command) and has MEF switching enabled. The **show gprs gtp pdp-context tid** command output displays some non zero values in the "MEF uplink packets / links" field.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list the caveats that have been resolved with Cisco LTE PGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d.

- Cisco LTE PGW Caveats, page 61
- Cisco SAMI Caveats, page 62

Cisco LTE PGW Caveats

This section lists the PGW caveats that are resolved with Cisco LTE PGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d.

- CSCtn10003

  When Remote Console and Logging (RCAL) is enabled on the Cisco Service and Application Module for IP (SAMI), the following error messages displays when a create context request is received, or a GTPv2 to GTPv1 handoff occurs on the PGW with the Radio Access Technology Type (RAT) type "5" (HSPA EVOLUTION):

  ```
  SAMI 1/4: Jun  8 04:47:42.859: %GTP-0-NORESOURCE: GSN: 0.0.0.0, TID: 00, APN: NULL,
  Reason: Invalid RAT value for recommended RAT IE
  ```

  The RAT type is set to null.

- CSCtq22874

  The Cisco SAMI running the Cisco LTE PGW Release 1.3.4 image might not generate service records as part of the call detail record (CDR) contents.

  This condition occurs when the PGW has a configuration under the APNs to generate local P-CDRs (**no service aware** command and **charging record type pcdr** command configuration), and there should be some PDP session establishments taking place with these APNs.

- CSCtq24403

  The active and standby gateways have a mismatch in the number of sessions after some create PDP context failures, or PDP contexts are deleted in the active gateway.

- CSCtq42159

  The Cisco LTE PGW might see constant high CPU usage (>90%) and could possibly not recover from that condition.

  This condition might occur when a GTPv0 create request is received on an existing GTPv1 PDP while that GTPv1 PDP is waiting to be deleted.

  When PDP contexts are being deleted at a high rate, some PDP contexts are in a delete pending queue waiting to be deleted. If a GTPv0 create request is received for one of these GTPv1 PDPs in the delete pending queue, the create request continuously gets enqueued for processing in a loop, and causes the high CPU on the PGW.

- CSCtq43085

  After a mediation device (MD) is attached to the Cisco LTE PGW, an "SNMP QFULL_ERR" error message is received if MD statistics are polled from the PGW.

  This condition occurs when the ifIndex on the Proxy Control Processor (PCOP) and Traffic and Control Plane processors (TCOPs) becomes out of sync when the **snmp-server ifindex persist** command is configure and interfaces are added or removed at the PCOP.

  When an MD attach occurs with the PCOP interface ifIndex, the MD entry is created at the PCOP. If the same ifIndex is not valid on the TCOPs, the MD creation fails at the TCOPs. Upon an MD statistics query, the PGW attempts to aggregate values per TCOP. Since the MD entry is not present at the TCOPs, they do not respond to the aggregation process, and the process times out after approximately 10 seconds. During this 10 second, a lot of SNMP packets are queued and queue overflow occurs, which results in a "SNMP QFULL_ERR" error.

- CSCtq440383

  The LTE SGW or LTE PGW might log "Active Charging Gateway NOT matching on Processors"

  This condition occurs when the Cisco SAMI is running the Cisco LTE SGW Release 1.x or the Cisco LTE PGW Release 1.x images.

- CSCtq71301

  An "INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0)" syslog message is generated on the standby SGW/PGW. This syslog message is a generic one and does not always indicate the issue.

  This condition occurs when more that 16384 paths are created (but do not necessarily exist simultaneously) and are synchronized to the standby gateway.

  If on the standby gateway, the **show gprs redundancy** command output displays a count more than 16384 in the Path Setup messages field, this is probably the issue.

Cisco SAMI Caveats

There are no Cisco SAMI caveats newly resolved with Cisco LTE PGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d.

Caveats - Cisco LTE PGW Release 1.3, Cisco IOS Release 12.4(24)T3c

This section contains open and resolved caveats that pertain to Cisco LTE PGW Release 1.3, Cisco IOS Release 12.4(24)T3c.

Open Caveats

Note Caveats open in one 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 LTE PGW Caveats

There are no known PGW caveats open in Cisco LTE PGW Release 1.3, Cisco IOS Release 12.4(24)T3c.

Cisco SAMI Caveats

This section lists the SAMI caveats that are open with Cisco LTE SPW Release 1.3, Cisco IOS Release 12.4(24)T3c.

- CSCti31555

  For dual stack sessions belonging to APNs with Mobile Express Forwarding (MEF) switching enabled, the “MEF uplink packets / links” field displays some non zero values immediately after the sessions come up.

  This condition occurs when sessions belonging to an APN, which has dual stack configured (using the **gtp bearer dual-addr** access-point configuration command) and has MEF switching enabled. The **show gprs gtp pdp-context tid** command output displays some non zero values in the “MEF uplink packets / links” field.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list the caveats that have been resolved with Cisco LTE PGW Release 1.3, Cisco IOS Release 12.4(24)T3c.

Cisco LTE PGW Caveats

This section lists the PGW caveats that are resolved with Cisco LTE PGW Release 1.3, Cisco IOS Release 12.4(24)T3c.

- CSCtj80560

  The Cisco LTE PGW crashes because of incorrect routing.

  Because of an increased latency in setting up a Policy and Charging Control (PCC) session, the SGSN performs a GTP version fallback from GTPv1 to GTPv0. In this scenario, the PGW attempts to clean up the pending GTPv1 session and create a GTPv0 context. While cleaning up the GTPv1 session, the PGW crashes.

- CSCtj99555

  The Cisco GGSN/Cisco LTE PGW crashes when an snmpwalk is made over cGtpPathStatisticsTable. This condition occurs when paths are created and removed (PDPs are created and deleted, or charging gateways are configured and unconfigured) during the snmpwalk.

- CSCtk75845

  Rulebase IDs are not synchronized between the active and standby PGWs.

  This condition occurs because the active PGWs sychronize the rulebase IDs only when the APNs are configured for service-aware charging. Therefore, rulebase IDs are not synchronized for APNs without the service-aware configuration.

- CSCtl93281

  The standby PGW crashes during a 4G session creation for an existing 3G session.

  This condition occurs when there is an existing GTPv1 session and the PGW receives a GTPv2 session with the same International Mobile Subscriber Identity (IMSI) and attempts to sychronize the newly arrived GTPv2 session to the standby PGW.

- CSCtl88898

  The Cisco LTE SGW and Cisco LTE PGW ignore the User Location Information (ULI) information element (IE) when it is sent in a delete session request.

- CSCtn08442

  The standby PGW crashes during the create IPv6 default and dedicated bearer process.

  This condition occurs when the rulebase IDs are sychronized from the active PGW to the standby PGW because of a null pointer access during the attribute decode.

- CSCtn12288

  An infinite loop causes the watchdog timer to reload the PGW.

  This condition occurs while the PGW is constructing a GTPv1 update response packet for a PDP on a service aware APN.

- CSCtn12329

  Traceback for a GTPv1 PDP update with service aware charging enabled.

  This condition occurs when service aware billing is configured and the PGW sends an update request to the SGSN and illegal memory access occurs.

- CSCtn14284

  An AAA access-request returns with an internal error, and on the Cisco GGSN or Cisco LTE PGW 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.

- CSCtn25629

  SNMP query for entPhysicalParentRelPos returns an incorrect value. This condition occurs because the SNMP query returns negative values because of an error in initialization of the data structure containing the processor details.

- CSCtn31609

  SNMP query for cpmCPUTotalPhysicalIndex returns an incorrect value. This condition occurs when the SNMP query is made for cpmCPUTotalPhysicalIndex 1, and an invalid value of 0 (zero) is returned instead of 2 because of an initialization error of the related table.

- CSCtn40983

  Crash occurs while executing a **show** command for a PDP that is in a deleting state.

  This condition occurs when the user issues a **show** command for a PDP that is already being deleted and waits on the "more" prompt while the contents of the PDP are deleted, and then continues with the **show** command, which attempts to access the freed PDP contents.

- CSCtn19492

  PDP becomes stuck when the RADIUS connection with the Cisco CSG2 is lost during the deleting state.

  This condition occurs when the reply from the Cisco CSG2 is delayed or lost.

Cisco SAMI Caveats

There are no Cisco SAMI caveats newly resolved with Cisco LTE PGW Release 1.2, Cisco IOS Release 12.4(24)T3c.

Caveats - Cisco LTE PGW Release 1.2, Cisco IOS Release 12.4(24)T3b

This section contains open and resolved caveats that pertain to Cisco LTE PGW Release 1.2, Cisco IOS Release 12.4(24)T3b.

Open Caveats

Note Caveats open in one 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 LTE PGW Caveats

There are no known Cisco LTE PGW caveats open in Cisco LTE PGW Release 1.2, Cisco IOS Release 12.4(24)T3b.

Cisco SAMI Caveats

This section lists the SAMI caveat that is open with Cisco LTE SPW Release 1.2, Cisco IOS Release 12.4(24)T3b.

- CSCti31555

  For dual stack sessions belonging to APNs with Mobile Express Forwarding (MEF) switching enabled, the "MEF uplink packets / links" field displays some non zero values immediately after the sessions come up.

  This condition occurs when sessions belonging to an APN, which has dual stack configured (using the **gtp bearer dual-addr** access-point configuration command) and has MEF switching enabled. The **show gprs gtp pdp-context tid** command output displays some non zero values in the "MEF uplink packets / links" field.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list the caveats that have been resolved with Cisco LTE PGW Release 1.2, Cisco IOS Release 12.4(24)T3b.

Cisco LTE PGW Caveats

This section lists the PGW caveats that are resolved with Cisco LTE PGW Release 1.2, Cisco IOS Release 12.4(24)T3b.

- CSCth54731

  During a GTPv2 to GTPv1 handoff, the radio access technology (RAT) type from the GTPv2 session is copied into the GTPv1 session without verifying if the GTPv2 RAT type is valid for the GTPv1 session. Therefore, the interim accounting messages are sent with an invalid RAT type for the GTPv1 session.

  This condition occurs when the RAT type is E-UTRAN and a handover from GTPv2 to GTPv1 occurs.

- CSCti93827

  The following error message displays on the console and some IPv6 addresses are not released into the pool after a session deletion, however, the addresses are assigned in subsequent session creations.

  ```
  IPC-3-SAMI_IPV6_POOL_FAIL: Unexpected condition: Malloc Failure for IPv6 Pool Mgmt
  Module
  ```

  This condition occurs when the Cisco LTE PGW is configured with 500 APNs, all of which have different VRFs and accounting and charging enabled, and the PGW receives continuous session create, modify, and delete requests at 750 calls per second (cps).

- CSCtj06869

  A Traffic and Control Plane Processor (TCOP) spikes for a long time during an SNMP query with 192K static traffic, 192K create/delete requests, and 192K create at 1200 cps.

  This condition occurs with the following sequence of events:

  a. Reload gateways
  b. Create 192K static dual-stack sessions with traffic
  c. Create/delete 192K at 1200CPS in a loop
  d. Create 192K at 120CPS with same International Mobile Subscriber Identity (IMSI) as in Step c
  e. On the SNMP server, do an **snmpwalk** and **getmany** on cGgsnExtMIB

  Issue the **show processor cpu** command to display that the Proxy Control Processor (PCOP) stays at 98% for a long time.

- CSCtj09958

  Some sessions are not synchronized to the standby Cisco LTE PGW when Gx is enabled for dual stack sessions with the DHCP option.

  When the PGW is configured with 500 APNs, all of which have different VRFs, Policy and Charging Control (PCC), accounting, charging, and DHCP proxy address allocation for IPv4 addresses, and redundancy configured, this condition occurs after approximately 38,000 sessions are created.

- CSCtj29343

  The Cisco LTE PGW reports that the Dynamic Feedback Protocol (DFP) high threshold has been reached and is congested due to low processor memory.

  This condition occurs after a switchover with 800K GTPv1 Gx sessions with charging enabled (time trigger set at five minutes and the volume trigger 1 Mb).

- CSCtj42310

  When the Cisco LTE PGW dynamically assigns IPv6 prefixes to the UEs from a local pool or from a RADIUS pool name or RADIUS prefix in response to a IPv6 router solicitation from the UE, the PGW must send an IPv6 router advertisement with the UE's prefix information with the lower 64 bits of the IPv6 address in the prefix extension set to zero. The PGW incorrectly sends the non zero UE's interface ID in the lower 64 bits.

  This condition occurs with an IPv6 solicitation from a UE using an IPv6 address.

- CSCtj45011

  Lawful Intercept does not intercept GTPv0 Intercept Related Information (IRI) and Content of Communication (CC) packets. A **show wire** issued on the Cisco LTE PGW displays that no packets are being intercepted for the generic stream. The mediation device (MD) also does not show any HI2_IRI or HI3_CC packets intercepted when context requests and date were sent to a specific International Mobile Subscriber Identity (IMSI) session.

- CSCtj79577

  When IPv6 primary and secondary DNS addresses are configured under an APN in the Active PGW, and an IPv6 session is created, the primary and secondary DNS addresses for that session are not synchronized to Standby PGW.

  This condition occurs when IPv6 DNS addresses are configured in the APN in the Active PGW, and an IPv6 session is synchronized to the Standby PGW.

- CSCtj83311

  The charging characteristics received in a GTPv2 message do no get synchronized from the Active to the Standby Cisco LTE PGW.

  This condition applies to all GTPv2 PDP contexts.

- CSCtk01630

  In compliance with the Release 8.2.0 Create Session Request, the first byte of the mobile station ISDN (MSISDN) number is removed.

- CSCtk05719

  Downstream traffic fails at the Cisco LTE PGW for IPv6 PDP contexts.

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

- CSCtk82421

  The Cisco LTE PGW clears the Autonomous bit while installing the MS prefix in the Interface Data Block (IDB), which causes the IPv6 ND RA message to be sent with the Autonomous bit not set.

  This condition occurs only when the UE requests dynamic IPv6 prefix allocation from the Cisco LTE PGW.

Cisco SAMI Caveats

This section lists the Cisco SAMI caveats that are resolved with Cisco LTE PGW Release 1.2, Cisco IOS Release 12.4(24)T3b.

- CSCth91677

  The UE is unable to acquire an IPv6 address.

  This condition occurs when the Cisco LTE PGW dynamically assigns IPv6 prefixes from the UEs from a local pool or from a RADIUS pool name or RADIUS prefix. The IPv6 router solicitation from the UE is lost and therefore, the UE is unable to acquire its IPv6 address.

- CSCti63031

  Data packets to or from the MSs are dropped for APNs with VRFs when IXP switching is enabled (the default).

  This condition occurs when the Cisco LTE PGW is configured with 500 APNs, all of which are configured with a different VRF and the **redirect all ip** command. Traffic for MSs from some of the 500 APNs is dropped at the IXP. The **show mef access-point** command displays an all zeros MAC address, for example, Redirect MAC Address: 0000.0000.0000.

- CSCti79332

  When the PGW is switching traffic at a high data rate (approximately 1.2 mpps) for more than 48 hours, the following error message along with a traceback is seen,

  ```
  %PLATFORM-3-SAMI_INTRHOG: DMA interrupt is running for (xxx)usecs, more than
  (xxx)usecs.
  ```

  This condition occurs when the PGW is connected to a Cisco CSG2 and there are 380K enabled sessions distributed over 500 APNs, all of which are configured with a different VRF, and the Gx and PCC features enabled, and the PGW is switching upstream and downstream data to these sessions at a high rate (1.2 million packets per second [mpps]) for more than 48 hours.

Caveats - Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1

This section contains open and resolved caveats that pertain to Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1.

Open Caveats

Note Caveats open in one 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 LTE PGW

The following PGW caveats are open in Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1.

- CSCti93827

  The following error message displays on the console and some IPv6 addresses are not released into the pool after a session deletion, however, the addresses are assigned in subsequent session creations.

  ```
  IPC-3-SAMI_IPV6_POOL_FAIL: Unexpected condition: Malloc Failure for IPv6 Pool Mgmt
  Module
  ```

  This condition occurs when the Cisco LTE PGW is configured with 500 APNs, all of which have different VRFs and accounting and charging enabled, and the PGW receives continuous session create, modify, and delete requests at 750 cps.

  Workaround: There is currently no known workaround, however, the addresses that were not deleted in the pool are not leaked since they are assigned to new users on subsequent session creations.

- CSCtj09958

  Some sessions are not synchronized to the standby PGW, when Gx is enabled for dual stack sessions with the DHCP option.

  When the PGW is configured with 500 APNs, all of which have VRF, Policy and Charging Control (PCC), accounting, charging, and DHCP proxy address allocation for IPv4 addresses, and redundancy configured, this condition occurs after approximately 38,000 sessions are created.

  Workaround: There is currently no known workaround.

Cisco SAMI

This section lists the SAMI caveats that are open with Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1.

- CSCti31555

  For dual stack sessions belonging to APNs with MEF switching enabled, “MEF uplink packets / links” field displays some non zero values immediately after the session comes up.

  This condition occurs when sessions belonging to an APN, which has dual stack configured (using the **gtp bearer dual-addr** access-point configuration command) and has MEF switching enabled (using the **redirect all ip** access-point command). The **show gprs gtp pdp-context tid** command output displays some non zero values in the “MEF uplink packets / links” field.

  Workaround: There is currently no known workaround.

- CSCti63031

  Data packets to or from the mobiles are dropped for APNs with VRF when IXP switching is enabled (the default).

  This condition occurs when the PGW is configured with 500 APNs, all of which are configured with a different VRF and the **redirect all ip** command. Traffic for mobiles from some of the 500 APNs is dropped at the IXP. The **show mef access-point** command displays an all zeros MAC address, for example, Redirect MAC Address: 0000.0000.0000.

  Workaround: Before any sessions are open for mobiles under an APN, issuing the **ping** command to the redirect addresses configured under the affected APNs triggers an Address Resolution Protocol (ARP) request that resolve the issue. Alternately, if there are a huge number of APNs with redirect addresses configured, saving the configuration and reloading the PGW resolves the issue.

- CSCti79332

  When the PGW is switching traffic at a high data rate (approximately 1.2 million packets per seconds [mpps]) for more than 48 hours, the following error message along with a traceback is seen,

  ```
  %PLATFORM-3-SAMI_INTRHOG: DMA interrupt is running for (xxx)usecs, more than
  (xxx)usecs.
  ```

  This condition occurs when the PGW is connected to a Cisco CSG2 and there are 380K enabled sessions distributed over 500 APNs, all of which are configured with a different VRF, and the Gx and PCC features enabled, and the PGW is switching upstream and downstream data to these sessions at a high rate (1.2 mpps) for more than 48 hours.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved with Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE PGW, page 70
- Cisco SAMI, page 70

Cisco LTE PGW

The following PGW caveats are resolved in Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1.

- CSCth24607

  A fatal error occurs on the active PGW after the virtual-template interface is modified and sessions are cleared using the **clear gprs gtp pdp-context** command.

- CSCth45430

  A traceback is seen on the Cisco LTE PGW. This condition occurs with downstream traffic greater than 1500 over IPv6 PDPs.

- CSCth52695

  The **show sami sm imsi** output fails to display existing PDP sessions. Additionally, after some time, the **gprs gtp pdp tid** command output also displays nothing.

  This condition occurs with IPv6 create requests with different restart counters.

- CSCth55339

  Tracebacks are observed with GTP Version 0 (GTPv0) PDPs on IPv6 transport handoffs to GTPv1 on IPv4 transport, and again with handoffs to GTPv0 on IPv4 transport.

  This condition occurs only when the handoff is between different IPv6/IPv4 transport.

Cisco SAMI

There are no SAMI caveats resolved with Cisco LTE PGW Release 1.1, Cisco IOS Release 12.4(24)T3a1.

Caveats - Cisco LTE PGW Release 1.0, Cisco IOS Release 12.4(24)T3a

This section contains the following types of caveats that pertain to Cisco LTE PGW Release 1.0, Cisco IOS Release 12.4(24)T3a.

Open Caveats—Cisco LTE PGW

This section documents possible unexpected behavior by Cisco LTE PGW Release 1.0, Cisco IOS Release 12.4(24)T3a and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCth20123

  Some sessions are deleted on the new standby PGW during the bulk synchronization after a switchover occurs.

  This condition occurs with IPv6 transport, and IPv6 neighbor discovery for the next hop fails for approximately three minutes after the reload.

  Workaround: Configure a static neighbor-to-IPv6 address mapping for the nexthop address for all GTP paths (for example **ipv6 1:1:1:1::1 GigabitEthernet0/0.100 0022.3344.5566**).

- CSCth24607

  A fatal error occurs on the active PGW after the virtual-template interface is modified and sessions are cleared using the **clear gprs gtp pdp-context** command.

  Workaround: There is currently no known workaround.

- CSCth45430

  A traceback is seen on the Cisco LTE PGW. This condition occurs with downstream traffic greater than 1500 over IPv6 PDPs.

  Workaround: There is currently no known workaround.

- CSCth52695

  The **show sami sm imsi** output fails to display existing PDP sessions. Additionally, after some time, the **gprs gtp pdp tid** command output also displays nothing.

  This condition occurs with IPv6 create requests with different restart counters.

  Workaround: There is currently no known workaround.

- CSCth55339

  Tracebacks are observed with GTP Version 0 (GTPv0) PDPs on IPv6 transport handoffs to GTPv1 on IPv4 transport, and again with handoffs to GTPv0 on IPv4 transport.

  This condition occurs only when the handoff is between different IPv6/IPv4 transport.

  Workaround: There is currently no known workaround.

Open Caveats—Cisco SAMI

This section lists the SAMI caveats that are open with Cisco LTE PGW Release 1.0, Cisco IOS Release 12.4(24)T3a.

- CSCtg64608

  The Cisco LTE gateway allows out of sequence traffic. This condition occurs when sending upstream traffic with the sequence number set to FFFF only with Mobile Express Forwarding (MEF). With Cisco Express Forwarding (CEF), the packets are dropped as designed.

  Workaround: Use CEF instead of MEF.

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 72
- Platform-Specific Documents, page 73
- •Cisco IOS Software Documentation Set, page 73

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 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**

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 LTE PGW Configuration Guide* and the *Cisco LTE PGW Command Reference* publications.