Release Notes for Cisco LTE Serving Gateway Release 1.3.7e on the Cisco SAMI, Cisco IOS Software Release 12.4(24)T35f

Latest Publication Date: July 30, 2012, Cisco IOS Release 12.4(24)T35f
Last Publication Date: July 6, 2012, Cisco IOS Release 12.4(24)T34f

This release note describes the requirements, dependencies, and caveats for the Cisco Long Term Evolution (LTE) Serving Gateway (SGW) 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 apply to the Cisco LTE SGW, Cisco IOS Releases 12.4(24)T3 releases, see the "Caveats" section on page 12 and *Caveats for Cisco IOS Release 12.4 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

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

Contents

This release note includes the following information:

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

Cisco LTE SGW Overview

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

LTE Evolved Packet Core

The Cisco LTE SGW 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.

The SAE is an 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.

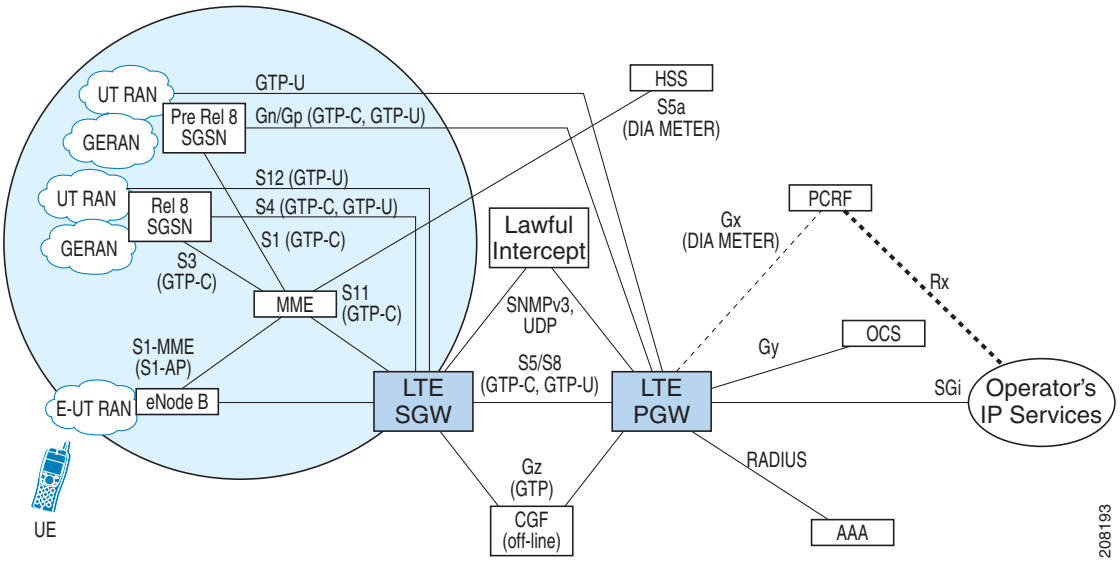
The LTE EPC is made up of the following primary elements:

- 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 represented by 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 SGW Description

For each UE associated with the EPS, there is a single SGW at any given time.

The Cisco LTE SGW Release 1.*x* supports GTP-based non-roaming and roaming architectures, and control and data plane functions defined by 3GPP TS 23.401 for 3GPP access networks.

The Cisco LTE SGW provides the following support:

- Routes and forwards data packets from the UE
- Terminates the interface towards Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)
- Mobility anchor point for inter-3GPP mobility (terminating S4 and relaying traffic between 2.5G/3G and LTE networks
- ECM-IDLE mode downlink packet buffering and initiation of network triggered service request procedure
- User traffic replication for Lawful Intercept
- Uplink (UL) and downlink (DL) charging per UE, packet data network (PDN), and quality of service (QoS) Class Identifier (QCI) (for example, for roaming with home-routed traffic)
- Handling of various messages between the MME, eNodeB, serving GPRS support node (SGSN), and PGW
- Processes both control and user plane messages

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

For more information about the Cisco SAMI, see the *Cisco Service and Application Module for IP User Guide*.

System Requirements

This section describes the system requirements for Cisco LTE SGW Release 1.*x* and includes the following sections:

- Memory Recommendations, page 5
- Hardware and Software Requirements, page 5
- Determining the Software Version, page 6
- Upgrading to a New Software Release, page 6

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 SGW Release 1.x

Platforms	Feature Sets	Software Image	Recommended Flash Memory (MB)	Recommended DRAM Memory (GB)	Runs From
Cisco SAMI, Cisco 7600	Cisco LTE SGW Standard Feature Set	c7svcsami-l4ik9s-mz	128	2	RAM

Hardware and Software Requirements

Implementing a Cisco LTE SGW Release 1.*x* on the Cisco 7600 series internet router platform requires the following hardware and software.

- Any module that has ports to connect to the network.
- A Cisco 7600 series router and one of the following supervisor engines running Cisco IOS Release 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 Cisco IOS Software required on the supervisor engine is dependent on the supervisor engine being used and the Cisco mobile wireless application running on the Cisco SAMI processors.

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

Note The Cisco LTE SGW 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:

```
SGW# show version
Cisco IOS Software, SAMI Software (SAMI-L3IK9S-M), 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)

SGW 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

...

SGW#
```

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 Serving Gateway Configuration Guide*.

Limitations, Restrictions, and Important Notes

When configuring the Cisco LTE SGW, note the following:

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

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

- The number of bearer/PDP contexts supported on a SGW is dependent on the memory and platform in use and the SGW configuration (for example, whether Dynamic Feedback Protocol [DFP] is being used or the memory protection feature is enabled, and what rate of bearer creation is supported).

  The Cisco LTE SGW on the Cisco SAMI with the 2-GB memory option can support 380000 PDN connections and the 380000 of default bearers. When the maximum allowable number of bearers/PDP contexts is reached, the SGW 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 delay period before the initialization of HSRP groups with the **standby delay minimum 100 reload 100** interface configuration command under the HRSP interface.
  - To minimize issues with high CPU usage for additional reasons, such as periods of high PPP PDP processing (creating and deleting), disable the notification of interface data link status changes on all virtual template interfaces of the SGW 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
    ```

New and Changed Information

The following sections document new features and behavior changes introduced in Cisco IOS Releases 12.4(24)T3 releases.

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

Cisco LTE SGW 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 This **show** command enhancement is identified by CSCts68540.

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 This **show tech** command enhancement is identified by CSCtt00301.

show gprs gtp statistics

The **show gprs gtp statistics** command output has been enhanced to include a "UP Req rejected for no S1-U (S) counter, which displays the number of times UBReq has been rejected at the SGW with no S1-U path.

Note This **show gprs gtp statistics** command enhancement is identified by CSCtt41315.

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 re-enable the monitor mechanism, use the **sami ixp monitor enable** command.

Note This new implementation is identified by CSCtt32257.

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

With Cisco LTE PGW Release 1.3.6, the following syslog messages have been introduced that identify a restart counter change has occurred that resulted in a particular MME being reloaded and the deletion of all contexts linked to that MME.

```
SAMI 3/4: %LTE_GTPV2-4-LTE_RESTART_COUNTER_CHANGED: GSN: 6.6.6.1, Sig src addr:
12.12.12.36, TID: 1111051000000021, MME: 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 SGW.
- 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.
- MME—IP address of the MME.
- Restart counter changed from *x* to *y*—Old and new restart count.

The traceback is harmless and associated with the syslog message.

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

Cisco LTE SGW Release 1.3, Cisco IOS Release 12.4(24)T3c introduces support for the 3GPP change request (CR) 278. CR 278 specifies that when the SGW receives an Error Indication either for a Radio Network Controller (RNC) or from an eNodeB, it sends a Downlink Data Notification message to the S4 SGSN or to the MME, respectively. (CSCtj66053)

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

In compliance with Release 8.2.0, the following behavior changes have been introduced in Cisco IOS Release 12.4(24)T3b.

- In the Create Session Request, the first byte of the mobile station ISDN (MSISDN) number is removed (CSCtk01630).
- If a charging reporting action is enabled on the Cisco LTE PGW, the Cisco LTE SGW forwards the information element (IE) in the Create Session Response to both the Mobility Management Entity (MME) and the serving GPRS support node (SGSN). Previously, per Release 8.1.1, the Cisco LTE SGW sent the IE only to the SGSN. (CSCtk82408)

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

Support for the following 3GPP specification CRs records for 29.274 has been introduced in Cisco LTE SGW 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 is disabled by default 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 11
- Creating a Remote Path Group, page 12

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 12.

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 the address of the remote node is configured and as well as the compliance profile to use.

	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

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 specific Cisco IOS Release 12.4(24)T3 release, on the Bug Toolkit page, use the **Software Version** drop down lists to select Cisco IOS Version 12.4(24)T3 release. To display information about a specific caveat, type the caveat number in the **Search for Bug ID** field.

This section contains the caveats for the following releases:

Caveats - Cisco LTE SGW Release 1.3.7e, Cisco IOS Release 12.4(24)T35f

This section lists the open, resolved and unreproducible caveats that pertain to Cisco LTE SGW Release 1.3.7d, Cisco IOS Release 12.4(24)T34f.

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 SGW Caveats, page 14
- Cisco SAMI Caveats, page 17

Cisco LTE SGW Caveats

The following Cisco LTE SGW caveats are open in Cisco IOS Release 12.4(24)T35f.

- CSCts34338

  The Cisco LTE SGW might drop 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.

- CSCts78873

  The Cisco LTE SGW Cisco Express Forwarding (CEF) packet drop counter increments.

  This condition occurs when the Cisco LTE SGW is configured to buffer packets. When configured to buffer packets, the SGW buffers packets on a per bearer basis. SGW buffering is limited to 20 packets per second (pps) per bearer. The SGW drops packets exceeding this rate, which causes the CEF packet drop counter to increment.

  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.

- CSCtu18533

  The Cisco LTE SGW reloads during the PDP clean up function.

  This reload occurs with the following conditions:

  - A dual APN, which is the same user, connects to multiple APNs with different EPS Bearer IDs (EBIs) and the same International Mobile Subscriber Identity (IMSI).
  - When a release access bearer request for a user is received that applies to both of the bearers.

  Workaround: There is currently no known workaround.

- CSCtu24144

  When polling of cGgsnExtSubscriberTable for GTPv2 calls, the trailing zeros of mobile station ISDN (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.

- CSCtu48751

  The Cisco LTE SGW does not send user location information (ULI) to the Cisco LTE PGW in the correct order. Therefore, the PGW sends incorrect ULI in P-CDRs.

  This condition occurs when the SGW receives multiple ULI types. The SGW parses the ULI correctly, however, it does not send the ULI to the PGW in the correct order.

  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.

- CSCtu86331

  The Cisco LTE SGW sends the incorrect PDP type in S-CDRs.

  This condition occurs after a GTPv1-to-GTPv2 handover. The PDN type is a conditional informational element (IE) in the create session request and is not sent from the MME in the create request for a GTPv1-to-GTPv2 handoff.

  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.

- CSCtw51035

  Spurious memory access or crash occurs when executing the **show gprs gtp pdp-context tid** command or the **show gprs gtp pdp-context imsi**.

  This condition occurs when the **show gprs gtp pdp-context** detailed output is waiting at the **automore** prompt, and a session or PDP context is modified by some control plane event that modifies or frees data structures.

  Workaround: Before executing the **show gprs gtp pdp-context** command, disable the Cisco IOS automore feature by executing the **terminal length 0** command in EXEC mode on the PCOP.

- CSCtw76665

  The Cisco LTE SGW sends a wild card "*" as the access point name in S-CDRs.

  This condition occurs when an access point name in a create session request does not match any access point name in the APN list configured on the SGW.

  Workaround: Configure all access point names to be used in the access point list.

- 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.

Cisco SAMI Caveats

The following Cisco SAMI caveats are open with Cisco IOS Release 12.4(24)T35f.

- 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 with Cisco LTE SGW Release 1.3.7e, Cisco IOS Release 12.4(24)T35f.

- Cisco LTE SGW Caveats, page 18
- Cisco SAMI Caveats, page 18

Cisco LTE SGW Caveats

The following Cisco LTE SGW caveat is resolved with Cisco IOS Release 12.4(24)T35f.

- CSCua38505

  The following syslog is observed on the standby SGW:

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

  This message appears if the Traffic and Control Plane processor (TCOP) path deletion synchronization is delayed at the same another TCOP begins sychronizing the same path. When this condition occurs, the existing path handle is overwritten by the new handle and the previous handle is not released, which causes an ID leak.

Cisco SAMI Caveats

There are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)T35f.

Caveats - Cisco LTE SGW Release 1.3.7d, Cisco IOS Release 12.4(24)T34f

This section lists the open, resolved and unreproducible caveats that pertain to Cisco LTE SGW Release 1.3.7d, Cisco IOS Release 12.4(24)T34f.

- Open Caveats, page 18
- Resolved Caveats, page 22

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 SGW Caveats, page 18
- Cisco SAMI Caveats, page 21

Cisco LTE SGW Caveats

The following Cisco LTE SGW caveats are open in Cisco IOS Release 12.4(24)T34f.

- CSCts34338

  The Cisco LTE SGW might drop 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.

- CSCts78873

  The Cisco LTE SGW Cisco Express Forwarding (CEF) packet drop counter increments.

  This condition occurs when the Cisco LTE SGW is configured to buffer packets. When configured to buffer packets, the SGW buffers packets on a per bearer basis. SGW buffering is limited to 20 packets per second (pps) per bearer. The SGW drops packets exceeding this rate, which causes the CEF packet drop counter to increment.

  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.

- CSCtu18533

  The Cisco LTE SGW reloads during the PDP clean up function.

  This reload occurs with the following conditions:

  – A dual APN, which is the same user, connects to multiple APNs with different EPS Bearer IDs (EBIs) and the same International Mobile Subscriber Identity (IMSI).

  – When a release access bearer request for a user is received that applies to both of the bearers.

  Workaround: There is currently no known workaround.

- CSCtu24144

  When polling of cGgsnExtSubscriberTable for GTPv2 calls, the trailing zeros of mobile station ISDN (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.

- CSCtu48751

  The Cisco LTE SGW does not send user location information (ULI) to the Cisco LTE PGW in the correct order. Therefore, the PGW sends incorrect ULI in P-CDRs.

  This condition occurs when the SGW receives multiple ULI types. The SGW parses the ULI correctly, however, it does not send the ULI to the PGW in the correct order.

  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.

- CSCtu86331

  The Cisco LTE SGW sends the incorrect PDP type in S-CDRs.

  This condition occurs after a GTPv1-to-GTPv2 handover. The PDN type is a conditional informational element (IE) in the create session request and is not sent from the MME in the create request for a GTPv1-to-GTPv2 handoff.

  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.

- CSCtw51035

  Spurious memory access or crash occurs when executing the **show gprs gtp pdp-context tid** command or the **show gprs gtp pdp-context imsi**.

  This condition occurs when the **show gprs gtp pdp-context** detailed output is waiting at the **automore** prompt, and a session or PDP context is modified by some control plane event that modifies or frees data structures.

  Workaround: Before executing the **show gprs gtp pdp-context** command, disable the Cisco IOS automore feature by executing the **terminal length 0** command in EXEC mode on the PCOP.

- CSCtw76665

  The Cisco LTE SGW sends a wild card "*" as the access point name in S-CDRs.

  This condition occurs when an access point name in a create session request does not match any access point name in the APN list configured on the SGW.

  Workaround: Configure all access point names to be used in the access point list.

- 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.

Cisco SAMI Caveats

The following Cisco SAMI caveats are open with Cisco IOS Release 12.4(24)T34f.

- 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 with Cisco LTE SGW Release 1.3.7d, Cisco IOS Release 12.4(24)T34f.

- Cisco LTE SGW Caveats, page 22
- Cisco SAMI Caveats, page 22

Cisco LTE SGW Caveats

There are no newly resolved Cisco LTE SGW caveats with Cisco IOS Release 12.4(24)T34f.

Cisco SAMI Caveats

There are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)T34f.

Caveats - Cisco LTE SGW 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 SGW 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 SGW Caveats, page 23
- Cisco SAMI Caveats, page 26

Cisco LTE SGW Caveats

The following Cisco LTE SGW caveats are open in Cisco LTE SGW Release 1.3.7c, Cisco IOS Release 12.4(24)T33f.

- CSCts34338

  The Cisco LTE SGW might drop 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.

- CSCts78873

  The Cisco LTE SGW Cisco Express Forwarding (CEF) packet drop counter increments.

  This condition occurs when the Cisco LTE SGW is configured to buffer packets. When configured to buffer packets, the SGW buffers packets on a per bearer basis. SGW buffering is limited to 20 packets per second (pps) per bearer. The SGW drops packets exceeding this rate, which causes the CEF packet drop counter to increment.

  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.

- CSCtu18533

  The Cisco LTE SGW reloads during the PDP clean up function.

  This reload occurs with the following conditions:

  – A dual APN, which is the same user, connects to multiple APNs with different EPS Bearer IDs (EBIs) and the same International Mobile Subscriber Identity (IMSI).

  – When a release access bearer request for a user is received that applies to both of the bearers.

  Workaround: There is currently no known workaround.

- CSCtu24144

  When polling of cGgsnExtSubscriberTable for GTPv2 calls, the trailing zeros of mobile station ISDN (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.

- CSCtu48751

  The Cisco LTE SGW does not send user location information (ULI) to the Cisco LTE PGW in the correct order. Therefore, the PGW sends incorrect ULI in P-CDRs.

  This condition occurs when the SGW receives multiple ULI types. The SGW parses the ULI correctly, however, it does not send the ULI to the PGW in the correct order.

  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.

- CSCtu86331

  The Cisco LTE SGW sends the incorrect PDP type in S-CDRs.

  This condition occurs after a GTPv1-to-GTPv2 handover. The PDN type is a conditional informational element (IE) in the create session request and is not sent from the MME in the create request for a GTPv1-to-GTPv2 handoff.

  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.

- CSCtw51035

  Spurious memory access or crash occurs when executing the **show gprs gtp pdp-context tid** command or the **show gprs gtp pdp-context imsi**.

  This condition occurs when the **show gprs gtp pdp-context** detailed output is waiting at the **automore** prompt, and a session or PDP context is modified by some control plane event that modifies or frees data structures.

  Workaround: Before executing the **show gprs gtp pdp-context** command, disable the Cisco IOS automore feature by executing the **terminal length 0** command in EXEC mode on the PCOP.

- CSCtw76665

  The Cisco LTE SGW sends a wild card "*" as the access point name in S-CDRs.

  This condition occurs when an access point name in a create session request does not match any access point name in the APN list configured on the SGW.

  Workaround: Configure all access point names to be used in the access point list.

- 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.

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 with Cisco LTE SGW Release 1.3.7c, Cisco IOS Release 12.4(24)T33f.

- Cisco LTE SGW Caveats, page 27
- Cisco SAMI Caveats, page 28

Cisco LTE SGW Caveats

This section list the SGW caveat that has been resolved in Cisco LTE SGW Release 1.3.7c, Cisco IOS Release 12.4(24)T33f.

- CSCtz30894

  The active Cisco LTE SGW crashes during the rare scenario in which an N3 x T3 transmission period timeout occurs for a Downlink Data Notification (DDN) message sent by the SGW to the MME at the same time a GTPv1-toGTPv2 handoff in progress for a session fails on the SGW.

  In detail, this crash occurs with the following scenario:

  a. A GTPv1 PDP exists on the PGW.
  b. The GTPv1 PDP is handed off to GTPv2 and the SGW receives a create session request (CSReq) from the Mobility Management Entity (MME) without an S1-U.
  c. The SGW sends an modify bearer request (MBReq) to the PGW. The PGW moves the session to GTPv2 and sends an modify bearer response (MBResp) to the SGW.
  d. The PGW begins to forward downlink data to the SGW.

e. While processing the MBResp, the SGW sends a DDN to the MME because of the downlink data.

f. The MBResp processing fails on the SGW and the session is deleted.

g. If the MME does not respond to the DDN and the T3 timer expires, the SGW crashes.

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 SGW 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 SGW Release 1.3.7b, Cisco IOS Release 12.4(24)T32f.

- Open Caveats, page 28
- Resolved Caveats, page 32
- 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 SGW Caveats, page 28
- Cisco SAMI Caveats, page 31

Cisco LTE SGW Caveats

The following Cisco LTE SGW caveats are open in Cisco LTE SGW Release 1.3.7b, Cisco IOS Release 12.4(24)T32f.

- CSCts34338

  The Cisco LTE SGW might drop 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.

- CSCts78873

  The Cisco LTE SGW Cisco Express Forwarding (CEF) packet drop counter increments.

  This condition occurs when the Cisco LTE SGW is configured to buffer packets. When configured to buffer packets, the SGW buffers packets on a per bearer basis. SGW buffering is limited to 20 packets per second (pps) per bearer. The SGW drops packets exceeding this rate, which causes the CEF packet drop counter to increment.

  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.

- CSCtu18533

  The Cisco LTE SGW reloads during the PDP clean up function.

  This reload occurs with the following conditions:

  – A dual APN, which is the same user, connects to multiple APNs with different EPS Bearer IDs (EBIs) and the same International Mobile Subscriber Identity (IMSI).

  – When a release access bearer request for a user is received that applies to both of the bearers.

  Workaround: There is currently no known workaround.

- CSCtu24144

  When polling of cGgsnExtSubscriberTable for GTPv2 calls, the trailing zeros of mobile station ISDN (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.

- CSCtu48751

  The Cisco LTE SGW does not send user location information (ULI) to the Cisco LTE PGW in the correct order. Therefore, the PGW sends incorrect ULI in P-CDRs.

  This condition occurs when the SGW receives multiple ULI types. The SGW parses the ULI correctly, however, it does not send the ULI to the PGW in the correct order.

  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.

- CSCtu86331

  The Cisco LTE SGW sends the incorrect PDP type in S-CDRs.

  This condition occurs after a GTPv1-to-GTPv2 handover. The PDN type is a conditional informational element (IE) in the create session request and is not sent from the MME in the create request for a GTPv1-to-GTPv2 handoff.

  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.

- CSCtw51035

  Spurious memory access or crash occurs when executing the **show gprs gtp pdp-context tid** command or the **show gprs gtp pdp-context imsi**.

  This condition occurs when the **show gprs gtp pdp-context** detailed output is waiting at the **automore** prompt, and a session or PDP context is modified by some control plane event that modifies or frees data structures.

  Workaround: Before executing the **show gprs gtp pdp-context** command, disable the Cisco IOS automore feature by executing the **terminal length 0** command in EXEC mode on the PCOP.

- CSCtw76665

  The Cisco LTE SGW sends a wild card "*" as the access point name in S-CDRs.

  This condition occurs when an access point name in a create session request does not match any access point name in the APN list configured on the SGW.

  Workaround: Configure all access point names to be used in the access point list.

- 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.

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 with Cisco LTE SGW Release 1.3.7b, Cisco IOS Release 12.4(24)T31f.

- Cisco LTE SGW Caveats, page 38
- Cisco SAMI Caveats, page 43

Cisco LTE SGW Caveats

This section lists the SGW caveats that are resolved in Cisco LTE SGW Release 1.3.7b, Cisco IOS Release 12.4(24)T32f.

- CSCty31897

  Cisco LTE SGW might not respond to a Modify Bearer Command message from Mobility Management Entity (MME).

  This happens when MME sends Modify Bearer Command request to the SGW as part of a 3G-to-4G handoff procedure. The SGW does not support the Modify Bearer Command message; therefore it might not might not respond to the message or might respond incorrectly.

Cisco SAMI Caveats

The following Cisco SAMI caveats are resolved with Cisco LTE SGW Release 1.3.7b, Cisco IOS Release 12.4(24)T32f.

- 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.

- 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.

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.

Caveats - Cisco LTE SGW 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 SGW 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 SGW Caveats, page 34
- Cisco SAMI Caveats, page 37

Cisco LTE SGW Caveats

The following Cisco LTE SGW caveats are open in Cisco LTE SGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

- CSCts34338

  The Cisco LTE SGW might drop 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.

- CSCts78873

  The Cisco LTE SGW Cisco Express Forwarding (CEF) packet drop counter increments.

  This condition occurs when the Cisco LTE SGW is configured to buffer packets. When configured to buffer packets, the SGW buffers packets on a per bearer basis. SGW buffering is limited to 20 packets per second (pps) per bearer. The SGW drops packets exceeding this rate, which causes the CEF packet drop counter to increment.

  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.

- 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.

- CSCtu18533

  The Cisco LTE SGW reloads during the PDP clean up function.

  This reload occurs with the following conditions:

  – A dual APN, which is the same user, connects to multiple APNs with different EPS Bearer IDs (EBIs) and the same International Mobile Subscriber Identity (IMSI).

  – When a release access bearer request for a user is received that applies to both of the bearers.

  Workaround: There is currently no known workaround.

- CSCtu24144

  When polling of cGgsnExtSubscriberTable for GTPv2 calls, the trailing zeros of mobile station ISDN (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.

- CSCtu48751

  The Cisco LTE SGW does not send user location information (ULI) to the Cisco LTE PGW in the correct order. Therefore, the PGW sends incorrect ULI in P-CDRs.

  This condition occurs when the SGW receives multiple ULI types. The SGW parses the ULI correctly, however, it does not send the ULI to the PGW in the correct order.

  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.

- CSCtu86331

  The Cisco LTE SGW sends the incorrect PDP type in S-CDRs.

  This condition occurs after a GTPv1-to-GTPv2 handover. The PDN type is a conditional informational element (IE) in the create session request and is not sent from the MME in the create request for a GTPv1-to-GTPv2 handoff.

  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.

- CSCtw51035

  Spurious memory access or crash occurs when executing the **show gprs gtp pdp-context tid** command or the **show gprs gtp pdp-context imsi**.

  This condition occurs when the **show gprs gtp pdp-context** detailed output is waiting at the **automore** prompt, and a session or PDP context is modified by some control plane event that modifies or frees data structures.

  Workaround: Before executing the **show gprs gtp pdp-context** command, disable the Cisco IOS automore feature by executing the **terminal length 0** command in EXEC mode on the PCOP.

- CSCtw76665

  The Cisco LTE SGW sends a wild card "*" as the access point name in S-CDRs.

  This condition occurs when an access point name in a create session request does not match any access point name in the APN list configured on the SGW.

  Workaround: Configure all access point names to be used in the access point list.

- 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.

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 SGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

- Cisco LTE SGW Caveats, page 38
- Cisco SAMI Caveats, page 43

Cisco LTE SGW Caveats

This section lists the SGW caveats that are resolved in Cisco LTE SGW Release 1.3.7a, Cisco IOS Release 12.4(24)T31f.

- CSCtu36084

  SGW call data records (SGW-CDRs) report more volume upload and download bytes than the PDN CDRs (PGW-CDRs) for the session.

  The following actions cause the S-CDR traffic volume count to be higher than the P-CDR service record count:

  a. Send user location information change via MBR for a GTPv2 session while the data is being sent continuously.

  b. Allow a few partial S-CDRs to be created.

  c. Clear the GTPv2 session.

- CSCtu40701

  The standby gateway reloads due to a Stream Control Transmission Protocol (SCTP) failure because of the interface queue of a Traffic and Control Plane processors TCOP reaches maximum capacity.

  This condition occurs when a lot of GTPv2-C messages are sent and the interface queue on the TCOP reaches the maximum value of 600. The queue fills for one of the following two reasons:

  a. A buffer leak for one session in a race condition.

  b. A lot of GTPv2-C messages are sent simultaneously for more than 10,000 sessions with a spike and the SGW is unable to process them and the queue builds to more than 600 packets for a few moments before clearing on its own.

- CSCtw72738

  On the Cisco LTE SGW, there might be a case when sending an Update Bearer Request (UBR) results in a a loop. This loop condition occurs when the UBR is rejected while a Re-Auth-Request (RAR) triggered UBR is retried and the S1-U is established, and subsequent UBRs are rejected.

- CSCtx05984

  The Cisco LTE SGW might reload when the eNodeB is not reachable during data path setup and the SGW is still trying to resolve the MAC, and the data path towards eNodeB is cleaned due to some other trigger such as a RAB or session deletion.

  This reload is seen only if an eNodeB is not reachable during path setup and at the same time, data path deletion is triggered by another even such as the receipt of a RAB or session deletion.

  Also, this reload occurs only if the time events are not handled in the correct sequence due to a TCOP processing a high load.

- CSCtx14133

  The S-CDR byte count is not correct.

  This condition occurs with the data bytes in a container closed with Cause for Record Closing.

Cisco SAMI Caveats

The following Cisco SAMI caveat is resolved with Cisco LTE SGW 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

Caveats - Cisco LTE SGW 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 SGW 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 SGW Caveats

The following Cisco LTE SGW caveats are open in Cisco LTE SGW Release 1.3.7, Cisco IOS Release 12.4(24)T3f.

- CSCts34338

  The Cisco LTE SGW might drop update PDP context requests because of an IMSI mandatory 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.

- CSCts78873

  The Cisco LTE SGW Cisco Express Forwarding (CEF) packet drop counter increments.

  This condition occurs when the Cisco LTE SGW is configured to buffer packets. When configured to buffer packets, the SGW buffers packets on a per bearer basis. SGW buffering is limited to 20 packets per second (pps) per bearer. The SGW drops packets exceeding this rate, which causes the CEF packet drop counter to increment.

  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.

- CSCtu18533

  The Cisco LTE SGW reloads during the PDP clean up function.

  This reload occurs with the following conditions:

  – A dual APN, which is the same user, connects to multiple APNs with different EPS Bearer IDs (EBIs) and the same International Mobile Subscriber Identity (IMSI).

  – When a release access bearer request for a user is received that applies to both of the bearers.

  Workaround: There is currently no known workaround.

- CSCtu21137

  RF-induced reloads are triggered by the TCOPs. This condition occurs in an Active/Standby redundant implementation.

  Workaround: There is currently no known workaround.

- CSCtu36084

  SGW call detail records (S-CDRs) report more volume upload and download bytes than the PDN CDRs (P-CDRs) for the session.

  The following actions cause the S-CDR traffic volume count to be higher than the P-CDR service record count:

  a. Send user location information change via MBR for a GTPv2 session while the data is being sent continuously.

  b. Allow a few partial S-CDRs to be created.

  c. Clear the GTPv2 session.

  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 SGW Release 1.3.7, Cisco IOS Release 12.4(24)T3f.

- Cisco LTE SGW Caveats, page 43
- Cisco SAMI Caveats, page 43

Cisco LTE SGW Caveats

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

- 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.

- CSCtt04252

  The mobile station ISDN (MSISDN) is not present in SGW call detail records (S-CDRs). This condition occurs after a 3G-to4G handoff.

- 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 SGW 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.

- 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 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.

- CSCtt42893

  The Cisco LTE SGW sends a modify bearer response with a cause code reserved value “0” when it receives a modify bearer request for an eNodeB update that does not contain User Location Information.

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

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 SGW Caveats

The following SGW caveat is open in Cisco LTE SGW Release 1.3.6, 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.

- CSCts78873

  The Cisco LTE SGW Cisco Express Forwarding (CEF) packet drop counter increments.

  This condition occurs when the Cisco LTE SGW is configured to buffer packets. When configured to buffer packets, the SGW buffers packets on a per bearer basis. SGW buffering is limited to 20 packets per second (pps) per bearer. The SGW drops packets exceeding this rate, which causes the CEF packet drop counter to increment.

  Workaround: There is currently no known workaround.

- CSCts95718

  The Cisco Mobile Wireless Transport Manager (MWTM) displays negative values for free memory.

  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 SGW Release 1.3.6, Cisco IOS Release 12.4(24)T3e.

- Cisco LTE SGW Caveats, page 46
- Cisco SAMI Caveats, page 47

Cisco LTE SGW Caveats

This section lists the SGW caveat that is resolved with Cisco LTE SGW Release 1.3.6, 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.

- CSCtr12187

  The PDP context becomes stuck on the Cisco LTE Serving Gateway (SGW).

  This condition occurs when a delete session request is sent to the Mobile Management Entity (MME) for the PDP when the SGW is waiting for a delete bearer response message from the MME.

- 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**.

Cisco SAMI Caveats

This section lists the Cisco SAMI caveats that are resolved with Cisco LTE SGW 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.

  The condition relates only 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 SGW 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 SGW Release 1.3.5, Cisco IOS Release 12.4(24)T35c.

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 SGW Caveats

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

- CSCtq81769

  Sessions remain stale in the Cisco LTE SGW.

  This condition occurs when a bearer resource create (BRC) is sent with a bidirectional traffic flow template (TFT) from the Mobility Management Entity (MME), and the SGW forwards the same to Cisco LTE PGW. The PGW rejects the BRC and replies to the SGW with bearer resource failure indication (BRFI). The SGW rejects the BRFI from the PGW.

  Workaround: Reconnect or perform a local clear on the SGW to remove the stale session.

Cisco SAMI Caveats

This section lists the SAMI caveats that are open with Cisco LTE SGW 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.

- CSCtk01565

  Mobile Express Forwarding (MEF) stops forwarding packets in the Cisco LTE SGW.

  This condition occurs when the Cisco LTE SGW receives a packet in which the inner IP packet is malformed. Specifically, the length field of the inner packet has a corrupted value.

  Workaround: Disable MEF using the **no mef** access-point configuration command.

Resolved Caveats

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

- Cisco LTE SGW Caveats, page 53
- Cisco SAMI Caveats, page 53
- Miscellaneous Caveats, page 51

Cisco LTE SGW Caveats

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

- 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.

- CSCtq57867

  In a redundant implementation, the requested APN Aggregate Maximum Bit Rate (APN-AMBR) values are not synced to the standby Cisco LTE SGW.

  This condition occurs when the session is created.

- CSCtq65935

  The Cisco LTE SGW crashes when a error indication is received from eNodeB/Radio Network Controller (RNC) for a dual-stack APN PDP context.

  This condition occurs when change request (CR) 278 of 3GPP TS 29.274 is enabled on the SGW by using the **cr** LTE compliance profile command, and the dual-stack session is deleted in the eNodeB/RNC and the SGW forwards downstream data to it.

- CSCtq70714

  A progressive memory leak occurs on the Cisco LTE SGW Proxy Control Processor (PCOP) when there is a Connection Set Identifier (CSID) delete PDP connection response failure received.

  ```
  5C79CCB4      148 45DB85BC  52   SingleIP PCOP S Single IP GGSN Parser
  0x45DB85BC:lte_singleip_sm_parse_gtp(0x45db8500)+0xbc
  ```

  This condition occurs when the SGW deletes a set of PDP contexts that have a common CSID and sends a delete PDN connection request to the Cisco LTE PGW. The PGW returns a negative response.

- CSCtq71187

  Downstream data traffic is sent to the Cisco LTE SGW instead of an SGSN when a GTPv1 to GTPv2 handover failure occurs because of Quality of Service (QoS).

  This condition occurs with the following sequence of events:

  1. A GTPv1 PDP context with streaming class is created.
  2. A GTPv1 to GTPv2 handoff request is sent to the SGW so that it sends a Maximum Bit Rate (MBR) to the Cisco LTE PGW.
  3. The converted QoS is used as QCI-4, which is Guarantee Bit Rate (GBR) bearer. Therefore, the PGW rejects the handover saying the default bearer can not be the GBR bearer and sends the packets to the SGW instead of the SGSN.

- CSCtq74189

  In a redundant implementation, a memory leak occurs on the active Cisco LTE SGW Traffic and Control Plane processors (TCOPs) after a couple of hours of continuous traffic and PDP context creates and deletes.

  This condition occurs when the path protocol to the charging gateway is TCP (**gprs charging path-protocol tcp**).

Cisco SAMI Caveats

This section lists the Cisco SAMI caveats that are resolved with Cisco LTE SGW 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.

- 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.

Miscellaneous Caveats

This section lists a miscellaneous Cisco IOS software caveat that is resolved with Cisco LTE SGW 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 a caveats that are unreproducible in Cisco LTE SGW 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 upon a reload at almost the same time of both gateways in a redundant implementation. This condition is more likely to occur when the Stream Control Transmission Protocol (SCTP) connectivity for the redundant configuration is lost.

- 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 TCOP CPU to become stuck at 99% usage.

  This issue is observed after a few hours under 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 to show 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 SGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d

This section contains open and resolved caveats that pertain to Cisco LTE SGW 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 SGW Caveats, page 52
- Cisco SAMI Caveats, page 52

Cisco LTE SGW Caveats

There are no known SGW caveats open in Cisco LTE SGW 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 SGW 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.

- CSCtk01565

  Mobile Express Forwarding (MEF) stops forwarding packets in the Cisco LTE SGW.

  This condition occurs when the Cisco LTE SGW receives a packet in which the inner IP packet is malformed. Specifically, the length field of the inner packet has a corrupted value.

  Workaround: Disable MEF using the **no mef** access-point configuration command.

Resolved Caveats

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

- Cisco LTE SGW Caveats, page 53
- Cisco SAMI Caveats, page 53

Cisco LTE SGW Caveats

This section lists the SGW caveat that is resolved with Cisco LTE SGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d.

- CSCtq44038

  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 SGW Release 1.3.4, Cisco IOS Release 12.4(24)T34d.

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

This section contains open and resolved caveats that pertain to Cisco LTE SGW 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 SGW Caveats

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

Cisco SAMI Caveats

This section lists the Cisco SAMI caveat that is open with Cisco LTE SGW Release 1.3, Cisco IOS Release 12.4(24)T3c.

- CSCtk01565

  Mobile Express Forwarding (MEF) stops forwarding packets in the Cisco LTE SGW.

  This condition occurs when the Cisco LTE SGW receives a packet in which the inner IP packet is malformed. Specifically, the length field of the inner packet has a corrupted value.

  Workaround: Disable MEF using the **no mef** access-point configuration command.

Resolved Caveats

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

Cisco LTE SGW Caveats

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

- CSCtl8889

  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.

- 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.

- CSCtn48330

  A crash occurs on the standby SGW when synchronizing SNMP MIB information. This condition occurs because MIB information is being synchronized from the PCOP and TCOPs when it should only be sychronized from the PCOP.

Cisco SAMI Caveats

There are no Cisco SAMI caveats newly resolved with Cisco LTE SGW Release 1.3, Cisco IOS Release 12.4(24)T3c.

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

This section contains open and resolved caveats that pertain to Cisco LTE SGW 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 SGW Caveats

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

Cisco SAMI Caveats

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

- CSCtk01565

  Mobile Express Forwarding (MEF) stops forwarding packets in the Cisco LTE SGW.

  This condition occurs when the Cisco LTE SGW receives a packet in which the inner IP packet is malformed. Specifically, the length field of the inner packet has a corrupted value.

  Workaround: Disable MEF using the **no mef** access-point configuration command.

Resolved Caveats

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

Cisco LTE SGW Caveats

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

- 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.

- CSCtk82409

  For dual-stack or IPv6 only sessions, the Cisco LTE SGW returns the prefix in the Create Session Request it received from the mobile management entity (MME) instead of sending the prefix length that Cisco LTE PGW returns in the Create Session Response.

  This condition occurs only when the UE uses dual-stack (IPv4 and IPv6) and IPv6 sessions.

Cisco SAMI Caveats

The following Cisco SAMI caveat is resolved with Cisco LTE SGW Release 1.2, Cisco IOS Release 12.4(24)T3b.

- 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.

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

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

- Open Caveats, page 56
- Resolved Caveats, page 57

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 SGW Caveats, page 56
- Cisco SAMI Caveats, page 56

Cisco LTE SGW Caveats

There are no known Cisco LTE SGW caveats open for Cisco LTE SGW Release 1.1, Cisco IOS Release 12.4(24)T3a1.

Cisco SAMI Caveats

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

- 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.

Resolved Caveats

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

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

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

- Open Caveats—Cisco LTE SGW, page 57
- Open Caveats—Cisco SAMI, page 57

Open Caveats—Cisco LTE SGW

There are no Cisco LTE SGW caveats open for Cisco IOS Release 12.4(24)T3a.

Open Caveats—Cisco SAMI

This section lists the SAMI caveats that are open with 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 58
- Platform-Specific Documents, page 58

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**

Note To view a list of MIBs supported by Cisco, by product, go to: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

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