Release Notes for Cisco LTE SPGW Gateway Release 2.*x* on the Cisco SAMI, Cisco IOS Software Release 12.4(24)T4 Releases

Latest Publication Date: September 23, 2013, Cisco IOS Release 12.4(24)T4o
Previous Publication Date: May 24, 2013, Cisco IOS Release 12.4(24)T4n

Cisco LTE SPGW Release 2.2.1m, Cisco IOS Release 12.4(24)T4o

This release note describes the requirements, dependencies, and caveats for the Cisco Long Term Evolution (LTE) Serving Gateway/PDN Gateway (SPGW) Release 2.*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 Cisco LTE SPGW, Cisco IOS Release 12.4(24)T4 releases, see the "Caveats" section on page 33 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.

Note Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.4* located on Cisco.com and with the *Cisco LTE SPGW Release 2.x Configuration Guide* and the *Cisco LTE SPGW Release 2.x Command Reference*.

Contents

This release note includes the following information:

Cisco Systems, Inc.
www.cisco.com

Cisco LTE SPGW Overview

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

LTE Evolved Packet Core

The Cisco LTE SPGW is a service designed for LTE Evolved Packet Core (EPC). The EPC is the main component of the System Architecture Evolution (SAE) that was designed by 3GPP to provide 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) core network 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)

Cisco LTE SPGW Description

The Cisco LTE SPGW is a Cisco IOS software feature that runs on the Cisco Service and Application Module for IP (SAMI) on the Cisco 7600 series platform. The Cisco LTE SPGW is a combined LTE serving gateway and LTE PDN gateway that 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 SPGW can service SGW-only, PGW-only, GGSN, or SPGW sessions.

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

Cisco LTE SPGW Release 2.0 and later supports all of the features and interfaces supported by the Cisco LTE PDN Gateway and Cisco LTE Serving Gateway Release 1.*x* and introduces the support for the following additional features:

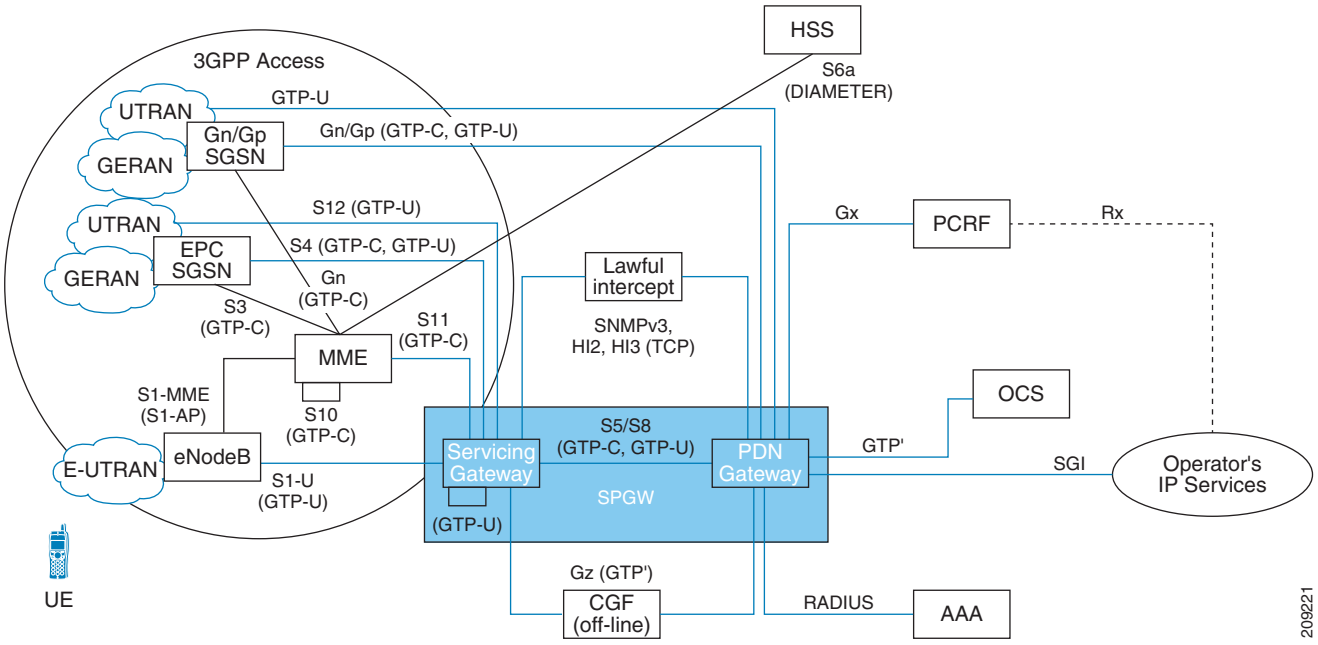
- 4 GB Cisco SAMI, which provides increased session and bearer density

- N:M ratio of SPGW to CSG2, where N is not equal to M, with associated load balancing between the SPGW and CSG2.
- Lawful Intercept based on mobile station ISDN (MSISDN) and International Mobile Equipment Identity (IMEI) subscriber selection
- Subscriber and equipment session tracing using an external Tracing Collection Entity (TCE)

Note Policy and Charging Enforcement Function (PCEF) and Gx functionality is provided by the Cisco Content Services Gateway - 2nd Generation (CSG2) running on a separate Cisco SAMI.

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

Figure 1 LTE Network Components and Interfaces with the Cisco LTE SPGW on the Cisco SAMI in the Cisco 7600 Series Router



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

- Serving GPRS Support Node (SGSN)
- 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)

System Requirements

This section describes the system requirements for Cisco LTE SPGW Release 2.*x* and includes the following sections:

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

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco LTE SPGW Release 2.x

Platforms	Feature Sets	Software Image	Recommended Flash Memory (MB)	Recommended DRAM Memory (GB)	Runs From
Cisco SAMI/ Cisco 7600	SPGW Standard Feature Set	c7svcsami-l3ik9s-mz	128	4	RAM

Hardware and Software Requirements

Implementing a Cisco LTE SPGW Release 2.*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 Multilayer 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 Multilayer Switch Feature Card (WS-SUP32-GE-3B) with LCP ROMMON Version 12.2(121) or later on the Cisco SAMI.
  - Cisco 7600 Series Supervisor Engine 32 with a Mutlilayer Switch Feature Card and 10 Gigabit Ethernet Uplinks (WS-SUP32-10GE-3B) with LCP ROMMON Version 12.2[121] or later on the Cisco SAMI.

Or one of the following Cisco 7600 series route switch processors running Cisco IOS Release 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) with the Cisco SAMI 4 GB memory option (Cisco Product Number: MEM-SAMI-6P-4GB[=]). The Cisco SAMI must be running Cisco IOS Release 12.4(24)T4a or later.
- For security, the IPSec VPN Services Module.
- For enhanced service-aware billing support, an additional Cisco SAMI running the Cisco Content Services Gateway Second Generation software in each Cisco 7600 series router.
- For GTP-Session Redundancy (GTP-SR):
  - 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:

```
SPGW# show version
Cisco IOS Software, SAMI Software (SAMI-L3IK9S-M), Version 12.4(24)T4
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Mon 28-January-13 09:49 by

ROM: System Bootstrap, Version 12.4(20100716:044940) [sopm-smbu_lte_r1_5-CSCtf55588 105],
DEVELOPMENT SOFTWARE

SPGW-Flash uptime is 22 hours, 14 minutes
System returned to ROM by reload at 22:43:43 UTC Mon January 28 2013
System restarted at 22:49:02 UTC Mon January 18 2013
System image file is "c7svcsami-l3ik9s-mz"
Last reload reason: Reload command by admin

...

SPGW#
```

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 Cisco SAMI PowerPCs (PPCs).

MIBs

To view a list of MIBs supported by Cisco IOS Release 12.4(24)T4 releases, see the *Cisco LTE SPGW Configuration Guide*.

Limitations, Restrictions, and Important Notes

When configuring the Cisco LTE SPGW, note the following:

- The Cisco LTE SPGW 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 the SPGW is dependent on the memory and platform in use and the SPGW configuration (for example, whether you are using Dynamic Feedback Protocol [DFP] or the memory protection feature is enabled) and the bearer creation rate.

  Table 2 lists the maximum number of sessions and bearers the Cisco SAMI with the 4 GB memory option can support:

Table 2 Number of Bearers/PDPs Supported in 4 GB SAMI

Session/Bearer Type	Maximum Number of Sessions
IPv4	846,000
IPv6	761,400
IPv4v6	761,400

Note When the maximum allowable number of bearers/PDP contexts is reached, the SPGW 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 HSRP interface.
  - To minimize issues with high CPU usage for additional reasons, such as periods of high PPP PDP processing (creating and deleting), disable the notification of interface data link status changes on all virtual template interfaces of the GGSN using the **no logging event link-status interface** configuration command.

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

- For Mobile Express Forwarding (MEF) support, you must configure the **redirect all** command or **aggregate** command under the APN.
- Ensure that **radius-server source ports extended** command is configured (to enable 200 ports in the range from 21645 to 21844 to be used as the source ports for sending out RADIUS requests). for more information about the **radius-server source ports extended** command, see the *Cisco IOS Security Command Reference*.
- Before executing the **show gprs gtp pdp-context tid** command in privileged EXEC mode, configure the Cisco LTE SPGW to not pause between multiple screens of output by using the **terminal length 0** command.

New and Changed Information

The following sections document new features and behavior changes that are introduced in a Cisco LTE SPGW Release 2.*x,* Cisco IOS Releases 12.4(24)T4 release. If a Cisco IOS Release 12.4(24)T4 release does not appear in this section, no new features or behavior changes were introduced in that release.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T4k

Cisco IOS Release 12.4(24)T4k introduces the following enhancements and behavior changes.

Retransmission Cache: Sequence Number Zero Handling for GTPv0 and GTPv1

Cisco IOS Release 12.2(24)T4k introduces the ability for operators to configure the Cisco LTE SPGW to ignore and not cache GTPv0 and GTPv1 messages for retransmission that contain zero (0) for a sequence number.

To configure the SPGW to ignore and not cache for retransmission GTPv0 and GTPv1 messages with a sequence number zero, use the following command in global configuration mode:

gprs gtp retransmit-ignore-seqno-zero ver {**0** | **1**}

Where:

- **0**—Configures the gateway to ignore GTPv0 messages with a sequence number zero.
- **1**—Configures the gateway to ignore GTPv1 messages with a sequence number zero.

By default, the gateway does not ignore GTP messages with a sequence number zero. To return to the default behavior, use the **no** form of this command.

When **gprs gtp retransmit-ignore-seqno-zero** command is configured, the gateway skips checking the retransmission cache functionality if the sequence number in a GTPv1 or GTPv0 message is zero.

(CSCud81844)

show Command Enhancements

With Cisco IOS 12.4(14)T4k, fields that formerly displayed in the **show gprs gtp pdp-context tid** command with restrictions now display without restriction. These fields are located in the Debug Info: section of the command output.

Additionally, the **show sami ixp hint** command has been added to the **show tech-support** command output and the **show sami ixp detail** command has replaced the s**how sami ixp statistics** command in the **show tech-support** command output.

(CSCud937325)

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T4j

Cisco IOS Release 12.4(24)T4j introduces the following changed behavior and enhancements:

Enhanced Description of Mobile Express Forwarding on the Cisco LTE SPGW

Mobile Express Forwarding (MEF), is when a Cisco SAMI network processors (IXP) performs packet switching for the mobile user data traffic.

By default, MEF is enabled on the Cisco LTE SPGW. You can disable MEF globally or at the APN level by using the **no mef** command. This configuration is NVGEN'd in the configuration.

MEF is applied independently on each bearer. For example, it is possible for some bearers in the gateway to be MEF-switched and other bearers to be CEF-switched.

Even when MEF is enabled globally, there are some configuration cases in which MEF is not enabled on the bearer. When this occurs, the Proxy Control Processor (PCOP) (also referred to as a PPC), using Cisco Express Forwarding (CEF) and process switching, handles data forwarding for these bearers.

The following scenarios are when the PPC handles data forwarding:

- The **no mef** command is configured under an APN. When **no mef** is configured in access-point configuration mode, all bearers connected to the APN are not MEF-switched.
- An extended Access Control List (ACL) is configured on an APN. When either an uplink or downlink ACL is configured, MEF is disabled for all bearers connected to the APN because the Cisco SAMI IXP cannot support protocol-based ACLs.

When MEF is enabled (the default), UE traffic and both uplink and downlink data traffic processed by the Cisco SAMI IXP. However, there are scenarios wherein the Cisco SAMI IXP sends packets to the PPC even when MEF is enabled. These scenarios include the following:

- If Lawful Intercept (LI) is enabled on the user. When LI is enabled, all traffic for that bearer is sent to the PPC because the Cisco SAMI IXP does not support the Cisco LTE SPGW LI feature. The user traffic is sent to the PPC so that PPC enforces the LI feature for the relevant bearer traffic in the CEF switching path. Once the LI is disabled for the bearer, the data traffic for the bearer is MEF-switched (handled by the Cisco SAMI IXP) once again.
- Downlink packets received when downlink data path is not ready (for example, due to a Radio Access Bearer [RAB]). When the downlink data path is not ready, the Cisco SAMI IXP sends the downlink packets to the PPC and the PPC buffers the packets (20 packets per second).
- Uplink packets that came when the MAC-to-CSG2 IP address is not yet resolved. When uplink packets are received when the MAC-to-CSG2 IP address is not resolved, the packets are sent to the PPC, and CEF punts the packet to the process path. The process path resolves the MAC-to-CSG2 IP address.
- When the Cisco SAMI IXP needs to drop an IPv4 packet that has the Don't Fragment (DF) bit set because of an MTU limitation. When the Cisco SAMI IXP needs to drop an IPv4 packet with the DF bit set because of an MTU limitation, the Cisco SAMI IXP sends the packet to the PPC. The PPC drops the packet and generates an Internet Control Message Protocol (ICMP) error response to the initial sender. The following two conditions are when this behavior occurs:
  - Uplink IPv4 UE packet, with the DF bit set, that is larger than the Gi interface IPv4 MTU is punted to PPC.
  - Downlink IPv4 packet, with DF bit set, that is larger than IPv4 session MTU (i.e. IPv4 MTU configured under Virtual-Template) is punted to PPC, and PPC drops the packet and sends an ICMP error response back to initial sender.
- Any packet that is larger than the MTU of the input interface (or the IPv4/IPv6 MTU as applicable). When a packet is larger than the MTU of the input interface, the packet is sent to PPC. This is common for both the uplink and downlink direction.
- Any packet that requires reassembly in the gateway. When a packet requires reassembly in the gateway, the packet is sent to the PPC. This occurs with the following three scenarios:
  - The uplink packet for a PGW- or SPGW-mode session where the outer IP packet (for example, GTP Transport Protocol Data Unit [TPDU] packet with GTP header encapsulation) is fragmented.
  - The uplink or downlink packet for a SGW-mode session where the outer IP packet (for example, GTP TPDU packet with GTP header encapsulation) is fragmented.

- Downlink IPv4 packet towards the UE, with DF bit set, that is larger than the IPv4 session MTU (for example, theIPv4 MTU configured under the Virtual-Template). When this occurs, the packet, is punted to the PPC and the PPC drops the packet and sends an ICMP error response back to the initial sender.
- Uplink IPv6 packet that is larger than the Gi interface MTU (for example, the IPv6 MTU configured under the relevant Gi sub-interface). When this occurs, the packet is punted to the PPC, and the PPC drops the packet and sends an ICMPv6 PktTooBig response back to the initial sender.
- Downlink IPv6 packet that is larger than the IPv6 session MTU (for example, the IPv6 MTU configured under the Virtual-Template). When a downlink IPv6 packet that is larger than the IPv6 session MTU occurs, the packet is punted to PPC, and PPC drops the packet and sends an ICMPv6 PktTooBig response back to the initial sender.
- Uplink IPv6 packet that is larger than the IPv6 session MTU (for example, the IPv6 MTU configured under Virtual-Template). When an uplink IPv6 packet that is larger than the IPv6 session MTU is received, the packet is punted to PPC and PPC handles the packet in CEF switching path.
- Uplink IPv4 packet, with DF bit not set, that is larger than the Gi interface IPv4 MTU. When an uplink IPv4 packet with the DF bit not set, that is larger than the GI interface IPv4 MTU is received, the gateway needs to fragment the uplink IPv4 packet. The Cisco SAMI IXP cannot fragment a packet and therefore, sends these packets to the PPC where CEF switching performs the fragmentation and forwards the packets to the Cisco CSG2.
- The Cisco SAMI IXP can only fragment a packet into two packets. If packet fragmentation requires more than two packets, the Cisco SAMI IXP forwards the packet to the PPC and the PPC performs the fragmentation in the CEF switching path.

  In the following two cases the Cisco IXP performs the fragmenting:

  - Downlink IPv4 packet larger than IPv4 session MTU (for example, the IPv4 MTU configured under Virtual-Template) without DF bit set.
  - Downlink IPv4 packet, after adding outer encapsulation (for example, GTP, UDP and outer-IP headers), becomes larger than the interface IPv4 MTU (for example, the IPv4 MTU configured under the relevant sub-interface or IPv6 interface if S1-U is over an IPv6 tunnel) without DF bit set.

New and Enhanced show Commands

To assist with understanding and debugging, additional counters for the various reasons for which data messages are dropped have been added to the **show gprs gtp statistics** command. Also, two new show commands, **show gprs gtp statistics cef** and **show gprs gtp statistics mef** are introduced in Cisco IOS Release 12.4(24)T4j that enable you to display separately the count of data messages dropped in the Cisco Express Forwarding (CEF) path and the Mobile Express Forwarding (MEF) path. (CSCub58176)

When viewing **show** command output, note the following:

- The counters that display in the **show gprs gtp statistics** command output are an aggregate of CEF and MEF drops.
- All of the error counters that display in the **show gprs gtp statistics** command output do not total the “Data msg dropped” because packets might be dropped for other reasons that are not accounted for.
- The fields that display in the command output vary depending on the features configured on the gateway.

For more information on the new and enhanced commands, see the following sections:

- show gprs gtp pdp-context, page 11

- show gprs gtp statistics, page 11
- show gprs gtp statistics cef, page 28
- show gprs gtp statistics mef, page 29

show gprs gtp pdp-context

To display PDPs by local control or data TEID, use the **show gprs gtp-context** command with the **teid** keyword option specified.

show gprs gtp pdp-context teid *value*

Example

```
Router# show gprs gtp pdp teid 4A100002
        TID              Mode   MS Addr    Source  Signaling Addr  APN
        3111111100000010 SGW    N/A                55.55.55.35     221g-gx.cisco.com
```

(CSCud66193)

show gprs gtp statistics

Use the **show gprs gtp statistics** command to display all packet drop reason counters:

```
Router# show gprs gtp statistics

LI statistics:
  HI2 packets sent  0                HI2 bytes sent 0
  HI3 packets sent  0                HI3 bytes sent 0

GTP statistics:
Error Causes:
  Version not supported      0            Msg too short              0
  Unknown msg                0            Unexpected sig msg         0
  Unexpected data msg        0            Unsupported comp exthdr    0
  Mandatory IE missing       0            Mandatory IE incorrect     0
  Optional IE invalid        0            IE unknown                 0
  IE out of order            0            IE unexpected              0
  IE duplicated              0            Optional IE incorrect      0
  PDP/bearer activation rejected (v0/v1/v2)     0
  TFT semantic error         0            TFT syntactic error        0
  Pkt filter semantic error  0            Pkt filter syntactic error 0
  PDP/bearer without TFT exist        0
  Non existent               0            Path failure               0
  No resource                0            Invalid length (t-pdu)     0
  Get pak_buffer failure     0            Sig msg dropped (v0/v1)    0
  Data msg dropped           0            Total msgs dropped         0
  Sig msg dropped (v2)       0            Invalid Length (v2)        0
  Reserved message value     0            Conditional IE missing     0
  Invalid reply from peer    0            Path restarted             0
  Downlink ACL failure       0            Uplink ACL failure         0
  Downlink QoS failure       0            Uplink QoS failure         0
  PDP check failure          0            PDP not found              0
  UL Data Msg rcvd in PCOP   0            UL Data Msg rcvd too early 0
  Data plane blocked         0
  CEF and process switch error 0
  Buffer data error           0           Invalid vaccess            0
  No interface or invalid key 0           No adjacency               0
  PDP suspended               0           Inner IP invalid           0
  PDP lock timed out          0           APN drop                   0
  Encapsulation error         0           Tunnel src ip error        0
  GTP seq error               0           MCB drop                   0
```

```
  PDP intercept               0           Global intercept           0
  Redirect MAC unresolved     0
Message Statistics:
  Rcvd v0/v1 signalling msg  1            Sent v0/v1 signalling msg  1
  Rcvd GTPv2 signalling msg  0
  Rcvd GTPv2 retransmits     0            Sent GTPv2 retransmits     0
  Rcvd PDU msg               0            Sent PDU msg               0
  Rcvd PDU bytes             0            Sent PDU bytes             0
GTP MEF statistics:
 SGW mode:
  Rcvd PDU msg             0      Sent PDU msg            0
 PGW mode:
  Rcvd PDU msg             0      Sent PDU msg            0
V0 statistics:
  Create context Req
      received    0             rejected    0
  Create context Res
      sent    0
  Update  context Req
      received    0             rejected    0
  Update  context Res
      sent    0
  Delete  context Req
      received    0             rejected    0
  Delete  context Res
      sent    0
V1 statistics:
  Create context Req
      received    0             rejected    0
  Create context Res
      sent    0
  Update  context Req
      received    0             rejected    0
  Update  context Res
      sent    0
  Delete  context Req
      received    0             rejected    0
  Delete  context Res
      sent    0
V2 statistics:
  Create Session Req
      received    0             sent    0            rejected    0
  Create Session Rsp
      received    0             sent    0            rejected    0
  Create Bearer Req
      received    0             sent    0            rejected    0
  Create Bearer Rsp
      received    0             sent    0            rejected    0
  Modify Bearer Req
      received    0             sent    0            rejected    0
  Modify Bearer Rsp
      received    0             sent    0            rejected    0
  Update Bearer Req
      received    0             sent    0            rejected    0
  Update Bearer Rsp
      received    0             sent    0            rejected    0
  Delete Session Req
      received    0             sent    0            rejected    0
  Delete Session Rsp
      received    0             sent    0            rejected    0
  Delete Bearer Req
      received    0             sent    0            rejected    0
  Delete Bearer Rsp
      received    0             sent    0            rejected    0
```

```
Change Notification Req
    received    0             sent    0            rejected    0
Change Notification Rsp
    received    0             sent    0            rejected    0
Modify Bearer Command
    received    0             sent    0            rejected    0
Modify Bearer Fail Ind
    received    0             sent    0            rejected    0
Delete Bearer Command
    received    0             sent    0            rejected    0
Delete Bearer Fail Ind
    received    0             sent    0            rejected    0
Bearer Resource Command
    received    0             sent    0            rejected    0
Bearer Resource Fail Ind
    received    0             sent    0            rejected    0
Release Access Bearer Req
    received    0             sent    0            rejected    0
Release Access Bearer Rsp
    received    0             sent    0            rejected    0
Trace Session Activation
    received    0             sent    0            rejected    0
Trace Session Deactivation
    received    0             sent    0            rejected    0
Downlink Data Notification
    sent        0
Downlink Data Notification Acknowledgement
    received    0             rejected    0
Downlink Data Notification Failure Indication
    received    0             rejected    0
Suspend Notification
    received    0             rejected    0
Suspend Acknowledge
    sent        0
Resume Notification
    received    0             rejected    0
Resume Acknowledge
    sent        0
Create Indirect Data Forwarding Tunnel Request
    received    0             rejected    0
Create Indirect Data Fowarding Tunnel Response
    sent        0
Delete Indirect Data Forwarding Tunnel Request
    received    0             rejected    0
Delete Indirect Data Fowarding Tunnel Response
    sent        0
Delete PDN Connection Set Request
    received    0             sent    0            rejected    0
Delete PDN Connection Set Response
    received    0             sent    0            rejected    0
Update PDN Connection Set Request
    sent    0
Update PDN Connection Set Response
    received    0            rejected    0
Stop Paging Indication
    sent        0
Echo Request
    received    0             sent    0            rejected    0
Echo Response
    received    0             sent    0            rejected    0
Version Not Supported(v2)
    received    0             sent    0            rejected    0
Error Indication(v1)
    received    0             sent    0
```

```
  Mandatory COA timeouts     0
Session handovers:
  P to SP change
      success    0             failed    0
  SP to P change
      success    0             failed    0
  P to GGSN change
      success    0             failed    0
  SP to GGSN change
      success    0             failed    0
  GGSN to P change
      success    0             failed    0
  GGSN to SP change
      success    0             failed    0
  v1 to v0 change
      success    0             failed    0
  v0 to v1 change
      success    0             failed    0
  eNB change
      success    0             failed    0
  MME change
      success    0             failed    0
  SGW data path change
      success    0             failed    0
  SGW ctrl path change
      success    0             failed    0

  Total created PDP/Bearers  0            Total deleted PDP/Bearers  0
  Total created PPP PDP      0            Total deleted PPP PDP      0
  Total created IT PDP       0            Total deleted IT PDP       0
  PPP regen pending          0            PPP regen pending peak     0
  PPP regen total drop       0
  PPP regen no resource      0            Ntwk init PDP act reject   0
  Total ntwkInit created PDP 0            Single PDP-session cleared 0
  Total ntwkInit update PDP  0            Total update responses rcv 0
  Total COA msg received     0            Total COA msgs discarded   0
  Total COA triggered update 0            Total err indications rcvd 0
  Total err indications sent 0            Number of times DT enabled 0
  Total EI rcvd on DT PDP/Bearers    0
  Total update fail DT PDP/Bearers   0
  Created IPv6 PDP           0            Rejected IPv6 PDP          0
  Deleted IPv6 PDP           0            Created IPv6 PDPMCB        0
  Deleted IPv6 PDPMCB        0            Rejected IPv4v6 PDP        0
  Created IPv4v6 PDP         0            Deleted IPv4v6 PDP         0
  Created IPv4v6 PDPMCB      0            Deleted IPv4v6 PDPMCB      0
  Rcvd IPv6 PDU              0            Sent IPv6 PDU              0
  Rcvd IPv6 data bytes       0            Sent IPv6 data bytes       0
  newinfo acct recs queued   0            newinfo acct recs failed   0
Echo stats:
 Charging:
  Request rcvd 1         Response sent 1
  Request sent 0         Response rcvd 0
 V0:
  Request rcvd 0         Response sent 0
  Request sent 0         Response rcvd 0
 V1:
  Request rcvd 0         Response sent 0
  Request sent 0         Response rcvd 0
Path stats:
 V0:
  Created 0          Deleted 0          Restarted 0
 V1 signaling:
  Created 0          Deleted 0          Restarted 0
 V1 data:
```

```
  Created 0          Deleted 0          Restarted 0
 V2 signaling:
  Created 0          Deleted 0          Restarted 0
Debug info:
  Path fail local del PDP    0            Ver upgrade local del      0
  No SGSN/SGW local del PDP  0            Ver fallback local del     0
  No wait SGSN/SGW local del PDP 0
  No req SGSN/SGW local del PDP  0
  Create collide with delete 0            Version changes            0
  Rcvd retransmit create req 0            Create as update           0
  PDP delete w/o close cause     0
  Del recd for del session    0     Incorrect Ref Count State  0
  Load Balance - No resource 0            Total collision detected   0
  PDP Punt due to High TFT   0
  Total v2 restart txn tmr expiry      0
  v2 restart txn exp with no PDP       0
  v2 restart txn exp with not v2 PDP   0
  Restart txn cancelled for other proc 0
  UBReq drop for no S1-U (SP) 0           UBReq rejected for no S1-U (S)  0
  CoA delayed for retry       0           Path Sync Create Over Create    0
  GTP len > Inner IP len (t-pdu)       0
  Retransmit cache expiry    60       seconds
  Rcvd GTPv0 retransmits     0
      Responded     0            Dropped     0
  Rcvd GTPv1 retransmits     0
      Responded     0            Dropped     0
  Rcvd GTPv2 retransmits     0
      Responded     0          Dropped     0
  Retransmission Cache Entries with Response        0
  Retransmission Cache Entries without Response     0
  Retransmission Cache Entries Timeout with Rsp     0
  Retransmission Cache Entries Timeout without Rsp  0
  Retransmission Cache Update Failures              0
  Process swicthed uplink pkts                      0
  Process swicthed downlink pkts                    0
Router#
```

Table 3 describes the fields that display in the **show gprs gtp statistics** command output.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
LI statistics:	Statistics related to Lawful Intercept (LI). **Note** These statistics display only when the PGW LI is enabled to send SNMP notifications for LI.
HI2 packets sent	Number of Intercept Related Information (IRI) packets sent over the HI2' interface.
HI2 bytes sent	Number of IRI bytes sent over the HI2' interface.
HI3 packets sent	Number of Content of Communication (CC) packets sent over the HI3' interface.
HI3 bytes sent	Number of CC bytes sent over the HI3' interface.
GTP statistics:	
Error Causes:	
Version not supported	Number of GTP messages received from devices running a GTP version other than GTPv0, GTPv1, or GTPv2.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
Msg too short	Number of GTP messages received that are too short to hold the GTP header for the supported GTP version.
Unknown msg	Number of unknown GTP messages received.
Unexpected sig msg	Number of unexpected GTP signaling messages received—for example, a message received on the wrong end of the tunnel or a response message received for a request that was not sent by the PGW.
Unexpected data msg	Number of GTP PDUs received for nonexistent PDPs/bearers.
Unsupported comp exthdr	Number of Create PDP Context requests received with unsupported extension headers when PGW comprehension is required.
Mandatory IE missing	Number of GTP messages received with a missing mandatory information element.
Mandatory IE incorrect	Number of GTP messages received with an incorrect mandatory information element—for example, with an IE that has an incorrect length.
Optional IE invalid	Number of GTP messages received with an IE that contains a value that is not within the defined range for that IE. GTP messages with invalid optional IEs are processed as if the IE was not present.
IE unknown	Number of GTP messages received with an information element of an unknown type.
IE out of order	Number of GTP messages received with an information element (IE) out of order.
IE unexpected	Number of GTP messages received with an information element that not expected in the GTP message, but is defined in GTP. GTP messages with unexpected IEs are processed as if the IE was not present.
IE duplicated	Number of GTP messages received with a duplicated information element.
Optional IE incorrect	Number of GTP messages received with an optional IE that is incorrect, which prevents the PGW from processing the GTP message correctly.
PDP/bearer activation rejected (v0/v1/v2)	Number of times a request to activate a PDP context or bearer session was rejected.
TFT semantic error	Number of GTP messages received with an IE with traffic flow template (TFT) semantic errors. A semantic error is when the defined format of the IE is valid but its content is inconsistent or invalid.
TFT syntactic error	Number of GTP messages received with an IE element with TFT syntactic errors. A syntactic error is when the coding of the IE is invalid.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
Pkt filter semantic_error	Number of GTP messages received with an IE with packet filter semantic errors. A semantic error is when the defined format of the IE is valid but the content of the IE is inconsistent or invalid.
Pkt filter syntactic error	Number of GTP messages received with an IE element with packet filter syntactic errors. A syntactic error is when the coding of the IE is invalid.
PDP/bearer w/o TFT exist	Number of create requests received without a traffic flow template information (TFT) IE.
Non existent	Number of create/update requests received for a session that does not exist on the gateway.
No resource	Number of times a resource was not available for creating a session. For example, the router may be out of memory.
Path failure	Number of path failures on the gateway.
Invalid length (t-pdu)	Number of TPDUs received with an invalid length in the header.
Get pak_buffer failure	Number of times the gateway has failed to allocate buffer for the GTP packet.
Sig msg dropped (v0/v1)	Number of GTPv0 and GTPv1 signaling messages dropped.
Data msg dropped	Number of GTP PDUs dropped.
Total msgs dropped	Number of GTP messages dropped.
Sig msg dropped (v2)	Number of GTPv2 signaling messages dropped.
Invalid Length (v2)	Number of GTPv2 signaling messages received with an invalid length.
Reserved message value	Number of GTP messages received with a cause IE with a reserved value.
Conditional IE missing	Number of GTP messages received with a conditional information element.
Invalid reply from peer	Number of GTP messages received with an invalid information element.
Path restarted	Number of GTP messages received with path restart count changed.
Downlink ACL failure	Number of downlink packets dropped by the gateway because of an ACL mismatch. This counter applies to all mode sessions in the downlink direction.
Uplink ACL failure	Number of uplink packets dropped by the gateway because of an ACL mismatch. This counter applies to all mode sessions in the uplink direction.
Downlink QoS failure	Number of downlink packets dropped by the gateway because of a QoS policing failure. This counter applies to all mode sessions in the downlink direction.
Uplink QoS failure	Number of uplink packets dropped by the gateway because of a QoS policing failure. This counter applies to all mode sessions in the uplink direction.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
PDP check failure	Number of packets dropped when the corresponding PDP is still not ready. This counter applies to all mode sessions in the downlink direction.
PDP not found	Number of packets dropped when the corresponding PDP is not found in the gateway.
UL Data Msg rcvd in PCOP	Number of data packets received on a controlled port. This counter applies to the uplink direction.
UL Data Msg rcvd too early	Number of packets dropped because the path is not ready yet. This counter applies to the uplink direction.
Data plane blocked	Number of packets dropped when the PDP is in a downlink blocked state and the data plane is not ready to switch traffic. This counter applies to all mode sessions in the downlink direction.
CEF and process switch error	Number of packets switching in CEF that failed and were punted to process level.
Buffer data error	Number of times a failure to buffer packet for a PDP has occurred. This counter applies to SGW and SPGW mode sessions in the downlink direction.
Invalid vaccess	Number of packets dropped because vaccess is not ready or the virtual template does not have an IP address.
No interface or invalid key	Number of packets dropped because no interface is found.
No adjacency	Number of packets dropped due to no adjacency found during switching. This counter applies to all mode sessions in the downlink direction.
PDP suspended	Number of packets received for a PDP that is in a suspended state.
Inner IP invalid	Number of sanity check failures on an inner packets IP version and length.
PDP lock time out	Number of times an attempt to lock on a PDP structure has failed.
APN drop	Number of packets dropped when intercept to drop packets is enabled on the APN.
Encapsulation error	Number of times a packet has been dropped because encapsulation has not been configured.
Tunnel src ip error	Number of times a packet data outer IP does not match the tunnel source IP when APN Tunnel Source Check is enabled. This counter applies to sessions in SGW mode in both directions.
GTP seq error	Number of times the GTP sequence number is not as expected. This counter applies to PGW and SPGW mode sessions in the uplink direction.
MCB drop	Number of packets dropped because intercept to drop packets is enabled on the MCB. This counter applies to PGW and SPGW mode sessions in the downlink direction.
PDP intercept	Number of packets dropped because intercept to drop packets is enabled on the PDP.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
Global intercept	Number of packets dropped because intercept is configured to drop. This counter applies to PGW and SPGW mode sessions in the uplink direction.
Redirect MAC unresolved	Number of packets dropped because the redirect MAC address could not be resolved. This counter applies to PGW and SPGW mode sessions in the uplink direction.
Message Statistics:	
Rcvd v0/v1 signalling msg	Number of GTPv0/v1 signaling messages received.
Sent v0/v1 signalling msg	Number of GTPv0/v1 signaling messages sent.
Rvd GTPv2 signalling msg	Number of GTPv2 signaling messages received.
Rcvd GTPv2 retransmits	Number of times the gateway received a retransmitted GTPv2 create session request. A retransmitted message is defined as a message with same GTP sequence number as the previous create request for a user.
Sent GTPv2 retransmits	Number of times the gateway sent a retransmitted GTPv2 create session request. A retransmitted message is defined as a message with same GTP sequence number as the previous create request for a user.
Rcvd PDU msg	Number of PDU messages received.
Sent PDU msg	Number of PDU messages sent.
Rcvd PDU bytes	Number of bytes received in PDUs.
Sent PDU bytes	Number of bytes sent in PDUs.
GTP MEF Statistics:	
SGW mode: Recvd PDU msg	Number of packets MEF-switched in SGW mode in the uplink direction.
SGW mode: Sent PDU msg	Number of packets MEF-switched in SGW mode in the downlink direction.
PGW mode: Recvd PDU msg	Number of packets MEF-switched in PGW, SPGW, and GGSN mode in the uplink direction.
PGW mode: Sent PDU msg	Number of packets MEF switched in PGW, SPGW, and GGSN mode in the uplink direction.
V0 Statistics:.	
Create Context Req received/rejected	Number of GTPv0 Create PDP Context Requests received and rejected.
Create Context Res received/rejected	Number of GTPv0 Create PDP Context Responses received and rejected.
Update context Req received/rejected	Number of GTPv0 Update PDP Context Requests received and rejected.
Update context Res received/rejected	Number of GTPv0 Update PDP Context Responses received and rejected.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
Delete context Req received/rejected	Number of GTPv0 Delete PDP Context Requests received and rejected.
Delete context Res sent	Number of GTPv0 Delete PDP Context Responses sent.
V1 Statistics:	
Create Context Req received/rejected	Number of GTPv1 Create PDP Context Requests received and rejected.
Create Context Res received/rejected	Number of GTPv1 Create PDP Context Responses received and rejected.
Update context Req received/rejected	Number of GTPv1 Update PDP Context Requests received and rejected.
Update context Res received/rejected	Number of GTPv1 Update PDP Context Responses received and rejected.
Delete context Req received/rejected	Number of GTPv1 Delete PDP Context Requests received and rejected.
Delete context Res sent	Number of GTPv1 Delete PDP Context Responses sent.
V2 Statistics:.	
Create Session Req received/sent/rejected	Number of Create Session Requests received, sent, and rejected.
Create Session Rsp received/sent/rejected	Number of Create Session Responses received, sent, and rejected.
Create Bearer Req received/sent/rejected	Number of Create Bearer Requests received, sent, and rejected.
Create Bearer Rsp received/sent/rejected	Number of Create Bearer Responses received, sent, and rejected.
Modify Bearer Req received/sent/rejected	Number of Modify Bearer Requests received, sent, and rejected.
Modify Bearer Rsp received/sent/rejected	Number of Modify Bearer Responses received, sent, and rejected.
Update Bearer Req received/sent/rejected	Number of Update Bearer Requests received, sent, and rejected.
Update Bearer Rsp received/sent/rejected	Number of Update Bearer Responses received, sent, and rejected.
Delete Session Req received/sent/rejected	Number of Delete Session Requests received, sent, and rejected.
Delete Session Rsp received/sent/rejected	Number of Delete Session Responses received, sent, and rejected.
Delete Bearer Req received/sent/rejected	Number of Delete Bearer Requests received, sent, and rejected.
Delete Bearer Rsp received/sent/rejected	Number of Delete Bearer Responses received, sent, and rejected.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
Change Notification Req received/sent/rejected	Number of Change Notification Requests received, sent, and rejected.
Change Notification Rsp received/sent/rejected	Number of Change Notification Responses received, sent, and rejected.
Modify Bearer Req received/sent/rejected	Number of Modify Bearer Requests received, sent, and rejected.
Modify Bearer Rsp received/sent/rejected	Number of Modify Bearer Responses received, sent, and rejected.
Delete Bearer Command received/sent/rejected	Number of Delete Bearer Commands received, sent, and rejected.
Delete Bearer Fail Ind received/sent/rejected	Number of Delete Bearer Fail Ind received, sent, and rejected.
Bearer Resource Command received/sent/rejected	Number of Bearer Resource Commands received, sent, and rejected.
Bearer Resource Fail Ind received/sent/rejected	Number of Bearer Resource Fail Indications received, sent, and rejected.
Release Access Bearer Req received/sent/rejected	Number of Release Access Bearer Requests received, sent, and rejected.
Release Access Bearer Rsp received/sent/rejected	Number of Release Access Bearer Responses received, sent, and rejected.
Trace Session Activation received/sent/rejected	Number of Trace Session Activations received, sent, and rejected.
Trace Session Deactivation received/sent/rejected	Number of Trace Session Deactivations received, sent, and rejected.
Downlink Data Notification sent	Number of Downlink Data Notifications sent.
Downlink Data Notification Acknowledgement received/rejected	Number of Downlink Data Notifications received and rejected.
Downlink Data Notification Failure Indication received/rejected	Number of Downlink Data Notifications sent.
Suspend Notification received/rejected	Number of Suspend Notifications received and rejected.
Suspend Acknowledge sent	Number of Suspend Acknowledgements sent.
Resume Notification received/rejected	Number of Resume Notifications received and rejected.
Resume Acknowledge sent	Number of Resume Acknowledgements sent.
Create Indirect Data Forwarding Tunnel Request received/rejected	Number Create Indirect Data Forwarding Requests received from the MME and the number rejected by the SPGW.
Create Indirect Data Forwarding Tunnel Response sent	Number Create Indirect Data Forwarding Requests received from the MME and the number rejected by the SPGW.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
Delete Indirect Data Forwarding Tunnel Request received/rejected	Number of Delete Indirect Data Forwarding Tunnel Requests received and rejected.
Delete Indirect Data Forwarding Tunnel Response sent	Number of Delete Indirect Data Forwarding Tunnel Responses sent.
Delete PDN Connection Set Request received/sent/rejected	Number of Delete PDN Connection Set Requests received and rejected.
Delete PDN Connection Set Response received/sent/rejected	Number of Delete PDN Connection Set Responses received and rejected.
Update PDN Connection Set Request sent	Number of Update PDN Connection Set Requests sent.
Update PDN Connection Set Response received/rejected	Number of Update PDN Connection Set Responses received and rejected.
Stop Paging Indication sent	Number of Stop Paging Indications sent.
Echo Request received/sent/rejected	Number of Echo Requests received, sent, and rejected.
Echo Response received/sent/rejected	Number of Echo Responses received, sent, and rejected.
Version not Supported (v2) received/sent/rejected	Number of Version not Supported Indications (GTPv2) received, sent, and rejected.
Error Indication (v1) received/sent	Number of Error Indications (GTPv1) sent.
Mandatory CoA timeouts	Number of times session creation fails due to a Change of Authorization (CoA) timeout. This counter is specific to GTPv2 as CoA is not mandatory for other PDP versions.
Session handovers:	
P to SP change success/failed	Number of PGW to SPGW mode session handovers that have succeeded and failed.
SP to P change success/failed	Number of SPGW to PGW mode session handovers that have succeeded and failed.
P to GGSN change success/failed	Number of PGW to GGSN mode session handovers that have succeeded and failed.
SP to GGSN change success/failed	Number of SPGW to GGSN mode session handovers that have succeeded and failed.
GGSN to P change success/failed	Number of GGSN to PGW mode session handovers that have succeeded and failed.
GGSN to SP change success/ failed	Number of GGSN to SP mode session handovers that have succeeded and failed.
v1 to v0 change success/failed	Number of GTPv1 to GTPv0 handovers that have succeeded and failed.
v0 to v1 change success/failed	Number of GTPv0 to GTPv1 handovers that have succeeded and failed.
eNB change success/failed	Number of eNodeB handoffs that have succeeded and failed.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
MME change success/failed	Number of MME handoffs that have succeeded and failed.
SGW data path change success/ failed	Number of SGW data path handoffs that have succeeded and failed.
SGW ctrl path change success/failed	Number of SGW control path handoffs that have succeeded and failed.
Total created PDP/Bearers	Number of PDP contexts/bearer sessions created since system startup (supports Special Mobile Group (SMG)-28 standards level and later)
Total deleted PDP/Bearers	Number of PDP contexts/bearer sessions deleted since system startup (supports SMG-28 standards level and later)
Total created PPP PDP	**Note** Not supported.
Total deleted PPP PDP	**Note** Not supported.
Total created IT PDP	Number of indirect tunnels created.
Total deleted IT PDP	Number of indirect tunnels deleted.
PPP regen pending	**Note** Not supported.
PPP regen pending peak	**Note** Not supported.
PPP regen total drop	**Note** Not supported.
PPP regen no resource	**Note** Not supported.
Ntwk init PDP act reject	Number of rejected PDP context requests that were initiated by the network (PDN). **Note** Not supported.
Total ntwkInit created PDP	Number of PDP context requests activated by the PGW that were initiated by the network (PDN). **Note** Not supported.
Single PDP-session cleared	Number of hanging PDP sessions cleared on the PGW. **Note** This counter is applicable only when an APN has a single pdp session configured.
Total ntwkInit update PDP	Number of Update PDP Context Requests sent by the PGW.
Total update responses rcv	Number of update request responses received.
Total COA msg received	Number of Change of Authorization (CoA) messages received on the PGW.
Total COA msgs discarded	Number of CoA messages discarded because of error.
Total COA triggered update	Number of GTPv1 Update PDP Context Requests and GTPv2 Update Bearer Requests initiated by the gateway because of a CoA trigger.
Total err indications rcvd	Number of error indications received on the PGW.
Total err indications sent	Number of error indications sent.
Number of times DT enabled	Number of direct tunnel PDP contexts established.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
Total EI rcvd on DT PDP/Bearers	Number of error indications sent from the radio network controller (RNC) received on the PGW for direct tunnel PDPs/bearers.
Total update fail DT PDP/Bearers	Number of direct tunnel PDPs/bearers deleted because the following reasons: • Direct Tunnel Update Context Request was responded to with a failure. • Failed to send Update Context Request for a direct tunnel PDP upon receiving an Error Indication message.
Created IPv6 PDP	Number of IPv6 PDPs created since system startup.
Rejected IPv6 PDP	Number of times an IPv6 create requests was rejected.
Deleted IPv6 PDP	Number of IPv6 PDPs deleted since system startup.
Created IPv6 PDPMCB	Number of IPv6 sessions created since system startup. One session can have one or more associated PDPs.
Deleted IPv6 PDPMCB	Number of IPv6 sessions deleted since system startup. One session can have one or more associated PDPs.
Rejected IPv4v6 PDP	Number of dual stack (IPv4v6) PDP create requests rejected since system startup.
Created IPv4v6 PDP	Number of IPv4v6 PDPs created since system startup.
Deleted IPv4v6 PDP	Number of IPv4v6 PDPs deleted since system startup.
Created IPv4v6 PDPMCB	Number of dual stack (IPv4v6) sessions created since system startup. One session can have one or more associated PDPs.
Deleted IPv4v6 PDPMCB	Number of dual stack (IPv4v6) sessions deleted since system startup. One session can have one or more associated PDPs.
Rcvd IPv6 PDU	Number of IPv6 PDU messages received.
Sent IPv6 PDU	Number of IPv6 PDU messages sent.
Rcvd IPv6 data bytes	Number of bytes received in IPv6 PDUs.
Sent IPv6 data bytes	Number of IPv6 PDU bytes sent.
newinfo acct recs queued	Number of Radius Accounting Message sent.
newinfo acct recs failed	Number of Radius Accounting Message failed.
Echo stats:	
Charging: Request rcvd	Number of charging gateway Echo requests received.
Charging: Request sent	Number of Echo responses sent to the charging gateway.
V0: Request rcvd	Number of GTPv0 Echo requests received.
V0: Request sent	Number of GTPv0 Echo responses sent.
V1: Request rcvd	Number of GTPv1 Echo requests received.
V1: Request sent	Number of GTPv1 Echo responses sent.
Path stats:	

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
V1 signaling:, V1 data:, V2 signaling:	
V0: Created	Number of GTPv0 paths created.
V0: Deleted	Number of GTPv0 paths deleted.
V0: restarted	Number of GTPv0 paths restarted.
V1 signaling: Created	Number of GTPv1 signaling paths created.
V1 signaling: Deleted	Number of GTPv1 signaling paths deleted.
V1 signaling: Restarted	Number of GTPv1 signaling paths restarted.
V1 data: Created	Number of GTPv1 data paths created.
V1 data: Deleted	Number of GTPv1 data paths deleted.
V1 data: Restarted	Number of GTPv1 data paths restarted.
V2 signaling: Created	Number of GTPv2 signaling paths created.
V2 signaling: Deleted	Number of GTPv2 signaling paths deleted.
V2 signaling: Restarted	Number of GTPv2 signaling paths restarted.
Debug info:	
Path fail local del PDP	Total number of PDPs deleted when a path failure is detected on a GTP path because one of the following conditions occurred: • The Echo Request sent to the peer did not receive a response before the N3 x T3 transmission period. • The restart counter of the peer node changed.
Ver upgrade local del	Number of GTPv0 PDPs deleted by the PGW when an SGSN sent a GTPv1 create request after a version upgrade.
No SGSN/SGW local del PDP	Number of times a PDP is deleted when the peer SGSN/SGW address is not present or valid. This situation might occur when PDPs are deleted because of one of following reasons: • The clear gprs gtp pdp-context command is issued to clear all PDPs. • The **clear gprs gtp pdp-context access-point** *access-point-number* is issued to clear all PDPs in an APN. • A half created PDP is deleted when the PGW has reached a low memory threshold.
Ver fallback local del	Number of GTPv1 PDPs deleted by the PGW when an SGSN sent a GTPv0 create request after a version fallback.
No wait SGSN/SGW local del PDP	Number of GTPv0, GTPv1, or GTPv2 PDPs deleted locally by the PGW after sending a delete context request or session request message to the peer SGSN/SGW before waiting for a response from the peer. This type of delete is usually triggered by issuing the **clear gprs gtp pdp access-point** *access-point-number* **no-wait-sgsn** command.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
No req SGSN/SGW local del PDP	Number of GTPv0, GTPv1, or GTPv2 PDPs deleted locally by the PGW without sending delete context request or delete session request to the peer SGSN/SGW. This type of delete is usually triggered by issuing the **clear gprs gtp pdp access-point** *access-point-number* **local** command.
Create collide with delete	Number of times a create context request is received for an existing GTPv0 or GTPv1 PDP when the existing PDP is already undergoing the deletion process. For GTPv2, it is the number of times a create session request is received for an existing GTPv2 PDP when the existing PDP is already undergoing the deletion process.
Version changes	Number of times a GTPv1 create context request was received for an existing GTPv0 PDP or a GTPv0 create context request was received for an existing GTPv1 PDP.
Rcvd retransmit create req	Number of times the gateway received a retransmitted GTPv1 or GTPv0 create context request or a GTPv2 create session request. A retransmitted message is defined as a message with the same GTP sequence number as the previous create request for a user.
Create as update	Number of times a GTPv1 or GTPv0 create context request for an existing PDP is treated as an update for the existing PDP. **Note** Not supported.
PDP delete w/o close cause	Number of times a GTPv0, GTPv1, or GTPv2 PDP attempts deletion without setting proper closure cause in the CDR. This is an error condition. In addition to incrementing this counter, the CDR closure cause is set to a default ABNORMAL_PDP_END.
Del recd for del session	Number of times a delete request is received for an existing GTPv0, GTPv1, or GTPv2 PDP that is already in the process of being deleted.
Incorrect Ref Count State	Number of times a GTPv0, GTPv1, or GTPv2 PDP has attempted to free while in an improper state.
Load Balance - No resource	**Note** Not supported.
Total collision detected	**Note** Not supported.
PDP punt due to High TFT	Number of packets punted from the Cisco SAMI IXP because of traffic flow template (TFT).
Total v2 restart txn tmr expiry	Number of times the backoff timer for an update bearer request retransmission has expired for a GTPv1 or GTPv0 PDP. This count indicates the number of times this timer was not stopped during a GTPv2-to-GTPv1 handoff.
v2 restart txn exp with no PDP	Number of times the backoff timer for an update bearer request retransmission has expired without a valid PDP associated with it. This count indicates the number of times this timer was not stopped during a GTPv2 PDP cleanup.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
v2 restart txn exp with no v2 PDP	Number of times the backoff timer for an update bearer request retransmission has expired for a GTPv1 or GTPv0 PDP. This count indicates the number of times this timer was not stopped during a GTPv2-to-GTPv1 handoff.
Restart txn cancelled for other proc	Number of time the backoff timer for an update bearer request retransmission is stopped while running because of an interim accounting request triggered by an event other than an update bearer response from SGW with cause code 110. The other events include: • Update bearer response from SGW with cause code other than 110. • Modify bearer request from SGW with any valid rating event.
UBReq drop for no S1-U (SP)	Number of times an Update Bearer Request was dropped because of a downlink block.
UBReq rejected for no S1-U (S)	Number of times Update Bearer Request was rejected because of a downlink block.
CoA delayed for retry	Number of times the SPGW halted sending an interim accounting message to the Cisco Content Services Gateway (CSG2) after an update bearer response was received from the SGW with cause code 110.
Path Synch Create Over Create	Number of times a path creation sync was received for an existing path on the standby gateway.
GTP len > Inner IP len (t-pdu)	Number of GTP packets received with a GTP length greater than the inner IP packet length.
Retransmit cache expiry	**Note** Not supported.
Rcvd GTPv0 retransmits Responded	Number of retransmitted GTPv0 messages that received a response.
Rcvd GTPv0 retransmits Dropped	Number of retransmitted GTPv0 messages dropped.
Rcvd GTPv1 retransmits Responded	Number of retransmitted GTPv1 messages that received a response.
Rcvd GTPv1 retransmits Dropped	Number of retransmitted GTPv1 messages dropped.
Rcvd GTPv2 retransmits Responded	Number of retransmitted GTPv2 messages that received a response.
Rcvd GTPv2 retransmits Dropped	Number of retransmitted GTPv2 messages dropped.
Retransmission Cache Entries with Response	**Note** Not supported.
Retransmission Cache Entries without Response	**Note** Not supported.
Retransmission Cache Entries Timeout with Response	**Note** Not supported.
Retransmission Cache Entries Timeout without Response	**Note** Not supported.

Table 3 show gprs gtp statistics Field Descriptions

Field	Description
Retransmission Cache Update Failures	**Note** Not supported.
Process switched uplink pkts	Number of uplink GTP data packets process switched.
Process switched downlink pkts	Number of downlink GTP data packets process switched.

show gprs gtp statistics cef

Use the **show gprs gtp statistics cef** command to display the CEF packet drop reason counters:

```
SPGW# show gprs gtp statistics cef
  Downlink packets received       0
  Uplink packets received         0
  Downlink bytes received         0
  Uplink bytes received           0

  Downlink ACL failure            0          Uplink ACL failure          0
  Downlink QoS failure            0          Uplink QoS failure          0
  PDP check failure               0          PDP not found               0
  Data plane blocked              0
  CEF and process switch error    0          No adjacency                0
  Buffer data error               0          Invalid vaccess             0
  No interface or invalid key     0          Unexpected data msg         0
  Uplink Data Msg rcvd in PCOP    0          Uplink T-PDU rcvd too early 0
  Msg too short                   0          Invalid length (t-pdu)      0

  Total Data msg dropped          0
SPGW#
```

Table 4 describes the fields that display in **show grps gtp cef** command output.

Table 4 show gprs gtp statistics cef Command Field Descriptions

Field	Description
Downlink packets received	Number of downlink packets received by the gateway.
Uplink packets received	Number of uplink packets received by the gateway.
Downlink bytes received	Number of downlink bytes received by the gateway.
Uplink bytes received	Number of uplink bytes received by the gateway.
Downlink ACL failure	Number of downlink packets dropped by the gateway because of an ACL mismatch.
Uplink ACL failure	Number of uplink packets dropped by the gateway because of an ACL mismatch.
Downlink QoS failure	Number of downlink packets dropped by the gateway because of QoS policing failure.
Uplink QoS failure	Number of uplink packets dropped by the gateway because of QoS policing failure.
PDP check failure	Number of packets dropped when the corresponding PDP is still not ready. This counter applies to the downlink direction.

Table 4 show gprs gtp statistics cef Command Field Descriptions

Field	Description
PDP not found	Number of packets dropped when the corresponding PDP is not found in the gateway.
Data plane blocked	Number of packets dropped when the PDP is in a downlink blocked state and the data plane is not ready to switch traffic. This counter applies to the downlink direction.
CEF and process switch error	Number of packets punted to process level because packet switching in CEF failed.
No adjacency	Number of packets dropped due to no adjacency found during switching. This counter applies to the downlink direction.
Invalid vaccess	Number of packets dropped as vaccess is not ready or the virtual template does not have an IP address.
Buffer data error	Number of packets failed to be buffered for a PDP. This counter applies SGW mode session in the downlink direction.
No interface or invalid key	Number of packets dropped when no interface is found.
Uplink Data Msg received in PCOP	Number of data packets received on the control port. This counter applies to the uplink direction.
Uplink Data Msg received too early	Number of packets dropped because the data path is not ready. This counter applies to the uplink direction.

show gprs gtp statistics mef

Use the **show gprs gtp statistics mef** command to display the MEF packet drop reason counters:

```
SPGW# show gprs gtp statistics mef
  Downlink ACL failure          0          Uplink ACL failure         0
  Downlink QoS failure          0          Uplink QoS failure         0
  PDP not found                 0          Redirect MAC unresolved    0
  Downlink PDP suspended        0          Uplink PDP suspended       0
  Downlink Inner IP invalid     0          Uplink Inner IP invalid    0
  Downlink PDP lock timed out   0          Uplink PDP lock timed out  0
  Downlink encap error          0          Uplink encap error         0
  Downlink tunnel src ip error  0          Uplink tunnel src ip error 0
  Downlink APN drop             0          Uplink APN drop            0
  Total Data Msg dropped        0
  GTP MEF statistics:
    SGW mode:
    Rcvd PDU msg              0       Sent PDU msg             0
    PGW mode:
    Rcvd PDU msg              0       Sent PDU msg             0
Router#
```

Table 5 describes the fields that display in this example.

Table 5 show gprs gtp statistics cef Command Field Descriptions

Field	Description
Downlink ACL failure	Number of downlink packets dropped by the gateway because of an ACL mismatch.
Uplink ACL failure	Number of uplink packets dropped by the gateway because of an ACL mismatch.
Downlink QoS failure	Number of downlink packets dropped by the gateway because of QoS policing failure.
Uplink QoS failure	Number of uplink packets dropped by the gateway because of QoS policing failure.
PDP not found	Number of packets dropped when the corresponding PDP is not found in the gateway.
Redirect MAC unresolved	Number of packets dropped because redirect MAC was not resolved.
Downlink PDP suspended	Number of packets dropped in downlink as corresponding PDP is suspended.
Uplink PDP suspended	Number of packets dropped in uplink as corresponding PDP is suspended.
Downlink Inner IP invalid	Number of times a sanity check failed for a downlink packet because of inner IP packet version and length.
Uplink Inner IP invalid	Number of times a sanity check failed for an uplink packet because of inner IP packet version and length.
Downlink PDP lock timed out	Number of attempts to get control to execute a PDP (lock) failed in the downlink direction.
Uplink PDP lock timed out	Number of attempts to get control to execute a PDP (lock) failed in the uplink direction.
Downlink encap error	Number of packets dropped in the downlink direction because encapsulation has not been configured.
Uplink encap error	Number of packets dropped in the uplink direction because encapsulation has not been configured.
Downlink tunnel src ip error	Number of uplink packets for which the data outer IP address does not match tunnel source IP address when APN Tunnel Source Check is enabled.
Uplink tunnel src ip error	Number of downlink packets for which the data outer IP address does not match tunnel source IP address when APN Tunnel Source Check is enabled.
Downlink APN drop	Number of packets dropped in downlink because intercept to drop packet is enabled for the APN.
Uplink APN drop	Number of packets dropped in uplink because intercept to drop packet is enabled for the APN.
Total Data Msg dropped	Number of packets dropped in the MEF path. **Note** The value for this counter might not be equal to the sum of all drop reasons because there might be other drop reasons.

Table 5 show gprs gtp statistics cef Command Field Descriptions

Field	Description
GTP MEF statistics:	
SGW mode: Rcvd PDU msg/Sent PDU msg	Number of packets switched in SGW mode.
PGW mode: Rcvd PDU msg/Sent PDU msg	Number of packets switched in PGW mode.

(CSCud05503)

IXP CSG Lookup Performance Changes

(CSCub43155)

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T4i

Cisco IOS Release 12.4(24)T4i introduces the following changed behavior and enhancements:

- The following informational syslog message has been added to log when the SGW information of a session is freed but not removed from the MME/SGSN path:

  ```
  %GTP-7-GTPPDPSTATE: GTP: PDP check: IMSI:211332000000000, MCBf:0x0, PDPf:0x0,
  MCB:0x4DAC0F8, LTE-MCB:0x5031010, MCB-SGW:0x5EA5358, MCB-PGW:0x50E2E50, PDP:0x0,
  LTE-PDP:0x0, NSAPI 0, SGW:0x0, PGW:0x0, Sig:0x0(NA), Data:0x0(NA)PDN mode:SPGW, HO old
  mode:NA, HO maj:NA, HO min:NA, SGW MME Path:0x0(Invalid), SGW SGSN Path:0x0(Invalid),
  Radio Path 1, Event Log: 0x3C2E2B393D19383B160000000000000000000000000000000000,
  ```

  (CSCuc25282)

- Prior to Cisco IOS Release 12.4(24)T4i, the APN name displayed in the **show gprs gtp pdp-context tid** command output was not consistent. For the CSR of a GTPv2 call, it displayed the Fully Qualified Domain Name (FQDN), but for a 3G-to4G handoff, the output displayed the APN name only.

  With Cisco IOS Release 12(24)T4i, the **show** command output displays only the APN name.

  (CSCuc17750)

- The following syslog message has been added and is logged in the active gateway when a session does not have sufficient buffer to copy session synchronizations information:

  ```
  %GPRSFLTMG-4-GPRS_RED_SYNC_BUFFER_OVERFLOW: SR encode buffer not enough to pack
  attribute
  ```

  (CSCuc21226)

- The **sgw** keyword option has been added to the **mef** command to enable MEF switching for SGW sessions. For example:

  ```
  Router(config)#mef ?
   imsi        Configure express forwarding for a imsi
   ixp         Configure express forwarding for an IXP
   ms-address  Configure express forwarding for a ms-address
   sgw         Configure express forwarding for SGW-Mode Sessions[Enabled on New
               Sessions]
  ...
  ```

(CSCuc23596)

- The **imsi multi-pdn** keyword option has been added to the **show gprs gtp pdp-context** command to display multi-PDN connections. Specifying the **imsi multi-pdn** keyword option displays the International Mobile Subscriber Identification (IMSI) number, number of connections, and the session mode. For example:

```
Router#show gprs gtp pdp imsi multi-pdn
IMSI               No. of Conn       Mode(NSAPI/LBI)
443344556611000       2             PGW(1) PGW(2)
443344556611001       2             PGW(1) PGW(2)
443344556611002       2             PGW(1) PGW(2)
```

(CSCuc21291)

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T4d

Cisco IOS Release 12.4(24)T4d introduces the following enhanced **show gprs gtp pdp-context** command output:

1. The session mode now indicates if a session is in a transient state of handover. An **[HO]** indicator is added to Mode field behind the existing mode of the session (PGW, SPGW or GGSN) to indicate the transient phase of handoff waiting on a message for handoff completion. The SGW-only mode does not have a transient phase.

```
SPGW-B# show gprs gtp pdp-context all
TID              Mode      MS Addr          Source  Signaling Addr  APN
1100010000000020 PGW[HO]   6.1.0.3          LOCAL   9.9.9.71        vrf.com1
```

Note The [HO] indicator applies to the **show gprs gtp pdp-context all** command output, the **show gprs gtp pdp-context tid** command output, and the **show gprs gtp pdp-context imsi** command output.

2. When a session is in a handoff transient state, the details of both the old path before the handoff and the new path after handoff are displayed in the **show gprs gtp pdp tid** command output.

```
SPGW-B# show gprs gtp pdp-context tid 1100010000000020
TID              Mode      MS Addr          Source  Signaling Addr  APN
1100010000000020 PGW[HO]   6.1.0.3          LOCAL   9.9.9.71        vrf.com1

    Current time: Feb 20 2012 05:34:29
    User name (IMSI): 110010000000000    MS address: 6.1.0.3
    MS International PSTN/ISDN Number (MSISDN): 2134567890123405
    IMEI : -

 Handover in progress: SP->P
   D/L Signaling Path switched: Y
   D/L Data Path switched: N
   Handover Status: Waiting on SM

 Old [Mode: SPGW] path details

 Interface: MME
    Signalling Address: 10.10.0.1
    Data Address:       9.9.9.71
    Control TEID local:  0x02200050
    Control TEID remote: 0x20000141
    Data TEID local:     0x82200052
    Data TEID remote:    0x4A100024
```

```
New [Mode: PGW] path details:
   SGW Addr signal: 9.9.9.71
   SGW Addr data:   9.9.9.71
   Control TEID local:  0x82200051
   Control TEID remote: 0x42100023
   Data TEID local:     0x82200052
   Data TEID remote:    0x4A100024
```

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T4b

Cisco IOS Release 12.4(24)T4b introduces support for the following:

- Enhanced compliance with 3rd Generation Project Partnership (3GPP) standard change requests (CRs).
- IMSI-based Subscriber and Equipment Session Tracing
- Enhanced ability to configure the charging data records (CDRs) generated by the Cisco LTE SPGW.

For more information about these enhancements, see the *Cisco LTE SPGW Release 2.1 Configuration Guide* and *Cisco LTE SPGW Release 2.1 Command Reference*.

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)T4a

Cisco IOS Release 12.4(24)T4a supports all of the features and interfaces the Cisco LTE PDN Gateway and Cisco LTE Serving Gateway Release 1.0 provide, plus introduces support for the following features:

- 4 GB Cisco SAMI, which provides increased session and bearer density
- IPv6 transport for RADIUS-based interfaces
- N:M ratio of SPGW to CSG2, where N is not equal to M, and with associated load balancing between the SPGW and CSG2.
- Lawful Intercept based on mobile station ISDN (MSISDN) and International Mobile Equipment Identity (IMEI) subscriber selection
- Subscriber and equipment session tracing using an external Tracing Collection Entity (TCE)

For a complete list of the features supported by the Cisco LTE PGW Release 1.*x* and Cisco LTE SGW Release 1.*x*, see the release notes for the Cisco IOS 12.4(24)T3c release of the Cisco LTE PGW and SGW.

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 the Cisco IOS Release 12.4(24)T4 releases.

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 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)T4 release, on the Bug Toolkit page, use the **Software Version** drop down lists to select Cisco IOS Version 12.4(24)T4 release. To display information about a specific caveat, type the caveat number in the **Search for Bug ID** field.

This section lists the following:

Caveats - Cisco IOS Release 12.4(24)T4o

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1m, Cisco IOS Release 12.4(24)T4o image:

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco SAMI Open Caveats, page 38

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4o.

- CSCtf14093

  Network Management System (NMS) poll on CISCO-IP-LOCAL-POOL-MIB does not provide IPv6 local pool entries.

  This condition is seen when an SNMP poll is done on CISCO-IP-LOCAL-POOL-MIB from Mobile Wireless Transport Manager (MWTM) or any other NMS. As a result of this condition, monitoring IPv6 local pools via an NMS not possible.

  Workaround: There is currently no known workaround.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCtz55440

  The QCI status counters that display in the **show gprs qos status** command output do not increment on the standby gateway after a session is deleted.

  This condition occurs with an active-standby gateway configuration when a PDP is created and the same PDP is deleted on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCub25920

  Some of the handover counters do not increment properly in the **show gprs gtp statistics** command output.

  This condition occurs with the following counters:

  – P to SP change
    failed 0

  - P to GGSN change
    success 0
  - SP to GGSN change
    success 0
  - GGSN to SP change
    failed 0

  Workaround: There is currently no known workaround.

- CSCub84708

  The value for the "Total activated EPS Idle Sessions" counter in the **show gprs gtp status** command output is much higher than the value for the "Total activated sessions" counter.

  The "Total activated EPS Idle Sessions" counter is incorrectly incremented or decremented when the following conditions occur:

  - A handoff cancellation.
  - DSR after an initial attach.
  - Handover request came in without data path info.

  Workaround: There is currently no known workaround.

- CSCuc02585

  The gateway crashes when flooded with Modify Bearer Requests.

  This condition occurs during continuous S4-to-S11 handoffs with mobility rate of 1200 when charging DRTs get rejected. Rejected DRTs leads to the accumulation of CDRs, and the memory occupied by the CDRs grows more than the limit, which results in the gateway crashing.

  Workaround: There is currently no known workaround.

- CSCuc11009

  The Cisco LTE SPGW crashes at "adj_switch_ipv4_generic_les" when processing downlink data packets.

  This condition occurs because of some inappropriate length in packet/calculations.

  Workaround: There is currently no known workaround.

- CSCuc30164

  The active Cisco LTE SPGW reloads with rate_limit_loop traceback. This condition occurs on the active SPGW during handovers with high data rates.

  Workaround: There is currently no known workaround.

- CSCuc84209

  The following syslog and traceback is seen on the active Cisco LTE SPGW:

```
SAMI 1/8: 000352: Oct 17 16:30:46: %GTP-7-GWDEBUG: PDP:0x065D100C, refcnt:0, Wrong
refcnt when charging_reserved,  -Traceback= 0x834586Cz 0x82C7004z 0x8054194z
0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000353: Oct 17 16:31:29: %ALIGN-3-SPURIOUS: Spurious memory access made at
0x82C5EC0z  reading 0xD4
SAMI 1/8: 000354: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C5EC0z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000355: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x8304178z 0x82C5F18z
0x82C6FE8z 0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz
SAMI 1/8: 000356: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C60A8z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
```

```
SAMI 1/8: 000357: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C6150z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000358: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x83456F0z 0x82C7004z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
```

The syslog and traceback is seen on active SPGW during the execution of the **show gprs gtp pdp-context tid all** command.

Workaround: There is currently no known workaround.

- CSCuc95775

  A crash is observed when deleting sessions.

  This condition occurs when DSR is sent with more calls per second (CPS) for approximately 150k sessions.

  Workaround: There is currently no known workaround.

- CSCud04444

  The Cisco LTE SPGW crashes with an unexpected exception to CPU.

  This condition is seen with an accounting feature after a prolonged stress test.

  Workaround: There is currently no known workaround.

- CSCud04466

  The Cisco LTE SPGW crashes due to an unexpected exception to CPU.

  This condition occurs with the Cisco IOS Cisco Express Forwarding (CEF) feature after prolonged stress conditions.

  Workaround: There is currently no known workaround.

- CSCud05773

  The Cisco LTE SPGW crashes with an Unexpected exception to CPU.

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCud24362

  A memory crash is seen while doing create/delete call-model tests with over 2.4 million UEs.

  Workaround: There is currently no known workaround.

- CSCud34267

  A crash occurs “@pak_has_particles (0x99eab9c)+0x4” during a 2.4M call model run.

  Workaround: There is currently no known workaround.

- CSCud09932

  The Cisco LTE SPGW crashes with “CPU exception.”

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCue20819

  Memory leaks are observed on the gateway under certain conditions.

  A PGW data Finite State Machine (FSM) leak is seen when there is a GTPv1 SP or P-SP handoff without establishing the data path. A GPRS list elem leak is seen when a create PDP fails on the standby gateway because of a resource issue.

Workaround: There is currently no known workaround.

- CSCuf00649

  The Cisco LTE SPGW crashes.

  While processing the SCU message from the Cisco CSG2, if the SPGW has an invalid PDP in the mcb structure, the gateway crashes.

  Workaround: There is currently no known workaround.

- CSCuf00799

  A Cisco LTE SPGW crash occurs with an accounting session ID traceback.

  This condition occurs when a stale session is present in the standby for the same transaction identifier (TID).

  Workaround: Reload the standby.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4o.

- 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 occasion 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.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

  Workaround: There is currently no known workaround.

- CSCua36249

  When an Xscale CPU reload occurs because of a QNX crash, the Cisco SAMI network processor (IXP) console displays the reload reason as UNKNOWN (IXP CAUSE = NP Core Reset - Cause Unknown).

  This condition occurs when there is a QNX microkernel crash on the Xscale CPU.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4o. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 39
- Cisco SAMI Resolved Caveats, page 39

Cisco LTE SPGW Resolved Caveats

The following SPGW caveat is resolved with Cisco IOS Release 12.4(24)T4o.

- CSCui81659

  The Data TPDU will be sent with wrong TEID (old TEID before Update Context request) by GW.

  When IP address of SGSN remains same with TEID of the Data Path, it alone changes on receiving update context request. It is applicable when traffic is MEF switched.

Cisco SAMI Resolved Caveats

The following Cisco SAMI caveat is resolved with Cisco IOS Release 12.4(24)T4o.

- CSCui37952

  Qos policing is not applied after 3G to 4G Handoff and vice versa. Customer was experiencing 4G speed data traffic in 3G call itself.

- CSCui57729

  Down Stream Ping Packets were not completely MEF Switched.

Caveats - Cisco IOS Release 12.4(24)T4n

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1k, Cisco IOS Release 12.4(24)T4n image:

- Open Caveats, page 39
- Resolved Caveats, page 43

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 39
- Cisco SAMI Open Caveats, page 43

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4n.

- CSCtf14093

  Network Management System (NMS) poll on CISCO-IP-LOCAL-POOL-MIB does not provide IPv6 local pool entries.

  This condition is seen when an SNMP poll is done on CISCO-IP-LOCAL-POOL-MIB from Mobile Wireless Transport Manager (MWTM) or any other NMS. As a result of this condition, monitoring IPv6 local pools via an NMS not possible.

  Workaround: There is currently no known workaround.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCtz55440

  The QCI status counters that display in the **show gprs qos status** command output do not increment on the standby gateway after a session is deleted.

  This condition occurs with an active-standby gateway configuration when a PDP is created and the same PDP is deleted on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCub25920

  Some of the handover counters do not increment properly in the **show gprs gtp statistics** command output.

  This condition occurs with the following counters:

  - P to SP change
    failed 0
  - P to GGSN change
    success 0
  - SP to GGSN change
    success 0
  - GGSN to SP change
    failed 0

  Workaround: There is currently no known workaround.

- CSCub84708

  The value for the “Total activated EPS Idle Sessions” counter in the **show gprs gtp status** command output is much higher than the value for the “Total activated sessions” counter.

  The “Total activated EPS Idle Sessions” counter is incorrectly incremented or decremented when the following conditions occur:

- A handoff cancellation.
- DSR after an initial attach.
- Handover request came in without data path info.

Workaround: There is currently no known workaround.

- CSCuc02585

  The gateway crashes when flooded with Modify Bearer Requests.

  This condition occurs during continuous S4-to-S11 handoffs with mobility rate of 1200 when charging DRTs get rejected. Rejected DRTs leads to the accumulation of CDRs, and the memory occupied by the CDRs grows more than the limit, which results in the gateway crashing.

  Workaround: There is currently no known workaround.

- CSCuc11009

  The Cisco LTE SPGW crashes at “adj_switch_ipv4_generic_les” when processing downlink data packets.

  This condition occurs because of some inappropriate length in packet/calculations.

  Workaround: There is currently no known workaround.

- CSCuc30164

  The active Cisco LTE SPGW reloads with rate_limit_loop traceback. This condition occurs on the active SPGW during handovers with high data rates.

  Workaround: There is currently no known workaround.

- CSCuc84209

  The following syslog and traceback is seen on the active Cisco LTE SPGW:

  ```
  SAMI 1/8: 000352: Oct 17 16:30:46: %GTP-7-GWDEBUG: PDP:0x065D100C, refcnt:0, Wrong
  refcnt when charging_reserved,  -Traceback= 0x834586Cz 0x82C7004z 0x8054194z
  0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000353: Oct 17 16:31:29: %ALIGN-3-SPURIOUS: Spurious memory access made at
  0x82C5EC0z  reading 0xD4
  SAMI 1/8: 000354: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C5EC0z 0x82C6FE8z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000355: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x8304178z 0x82C5F18z
  0x82C6FE8z 0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz
  SAMI 1/8: 000356: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C60A8z 0x82C6FE8z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000357: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C6150z 0x82C6FE8z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000358: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x83456F0z 0x82C7004z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  ```

  The syslog and traceback is seen on active SPGW during the execution of the **show gprs gtp pdp-context tid all** command.

  Workaround: There is currently no known workaround.

- CSCuc95775

  A crash is observed when deleting sessions.

  This condition occurs when DSR is sent with more calls per second (CPS) for approximately 150k sessions.

  Workaround: There is currently no known workaround.

- CSCud04444

The Cisco LTE SPGW crashes with an unexpected exception to CPU.

This condition is seen with an accounting feature after a prolonged stress test.

Workaround: There is currently no known workaround.

- CSCud04466

  The Cisco LTE SPGW crashes due to an unexpected exception to CPU.

  This condition occurs with the Cisco IOS Cisco Express Forwarding (CEF) feature after prolonged stress conditions.

  Workaround: There is currently no known workaround.

- CSCud05773

  The Cisco LTE SPGW crashes with an Unexpected exception to CPU.

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCud24362

  A memory crash is seen while doing create/delete call-model tests with over 2.4 million UEs.

  Workaround: There is currently no known workaround.

- CSCud34267

  A crash occurs "@pak_has_particles (0x99eab9c)+0x4" during a 2.4M call model run.

  Workaround: There is currently no known workaround.

- CSCud09932

  The Cisco LTE SPGW crashes with "CPU exception."

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCue20819

  Memory leaks are observed on the gateway under certain conditions.

  A PGW data Finite State Machine (FSM) leak is seen when there is a GTPv1 SP or P-SP handoff without establishing the data path. A GPRS list elem leak is seen when a create PDP fails on the standby gateway because of a resource issue.

  Workaround: There is currently no known workaround.

- CSCuf00649

  The Cisco LTE SPGW crashes.

  While processing the SCU message from the Cisco CSG2, if the SPGW has an invalid PDP in the mcb structure, the gateway crashes.

  Workaround: There is currently no known workaround.

- CSCuf00799

  A Cisco LTE SPGW crash occurs with an accounting session ID traceback.

  This condition occurs when a stale session is present in the standby for the same transaction identifier (TID).

  Workaround: Reload the standby.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4n.

- 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 occasion 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.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

  Workaround: There is currently no known workaround.

- CSCua36249

  When an Xscale CPU reload occurs because of a QNX crash, the Cisco SAMI network processor (IXP) console displays the reload reason as UNKNOWN (IXP CAUSE = NP Core Reset - Cause Unknown).

  This condition occurs when there is a QNX microkernel crash on the Xscale CPU.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4n. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 43
- Cisco SAMI Resolved Caveats, page 44

Cisco LTE SPGW Resolved Caveats

The following SPGW caveat is resolved with Cisco IOS Release 12.4(24)T4n.

- CSCuf76872

  There is a mobility stream "Stuck" in the mobility Stream Table (cmtapStreamTable). Two mobility streams for each user, one for IRI and another one for CC, need to be created and provisioned more than 1000 users. The number of mobility stream created would be 2000.

- CSCug58396

  "Out of IDs" syslog is seen on active SPGW.

  This condition occurs when SPGW allocates an ID for each path and PDPs that are created on GW.

This ID is used by SPGW's redundancy mechanism during syncing path and/or PDP to standby. Due to a software bug in SPGW, such IDs are not released when a GTPv0/v1 signaling or data path is deleted. If there are a lot of GTPv0/v1 path deletions, then these IDs can get exhausted after a long period of uptime. Once these IDs are exhausted, newly created paths on active are not properly synced to standby.

- CSCug65535

  The Calea MD is unable to see the updated APN AMBR value.

  This condition occurs if there is a change in APN AMBR value after the initial session creation.

- CSCug44933

  GPRS Charging Transfer process takes 90% CPU under rare circumstances.

  GPRS Charging Transfer process is responsible for transferring all closed CDRs to Charging Gateway. Under a certain circumstance, this process can enter into an infinite loop while trying to send out a specific CDR. This results in high CPU.

- CSCue56496

  A memory leak occurs in standby gateway. Chunk name is "SGW FSM Param."

  This condition occurs when the dataplane is modified because of a MBR received without data FTEID.

- CSCug94997

  The GPRS Charging Transfer process consumes high CPU on active SPGW.

  GPRS Charging Transfer process is responsible for transferring all closed CDRs to Charging Gateway. Under certain circumstances, this process can enter into an infinite loop while trying to send out a specific CDR. This results in high CPU.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI-specific caveats in Cisco IOS Release 12.4(24)T4n.

Caveats - Cisco IOS Release 12.4(24)T4m

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1j, Cisco IOS Release 12.4(24)T4m image:

- Open Caveats, page 44
- Resolved Caveats, page 49

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 45
- Cisco SAMI Open Caveats, page 48

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4m.

- CSCtf14093

  Network Management System (NMS) poll on CISCO-IP-LOCAL-POOL-MIB does not provide IPv6 local pool entries.

  This condition is seen when an SNMP poll is done on CISCO-IP-LOCAL-POOL-MIB from Mobile Wireless Transport Manager (MWTM) or any other NMS. As a result of this condition, monitoring IPv6 local pools via an NMS not possible.

  Workaround: There is currently no known workaround.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCtz55440

  The QCI status counters that display in the **show gprs qos status** command output do not increment on the standby gateway after a session is deleted.

  This condition occurs with an active-standby gateway configuration when a PDP is created and the same PDP is deleted on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCub25920

  Some of the handover counters do not increment properly in the **show gprs gtp statistics** command output.

  This condition occurs with the following counters:

  - P to SP change
    failed 0
  - P to GGSN change
    success 0

  - SP to GGSN change
    success 0
  - GGSN to SP change
    failed 0

  Workaround: There is currently no known workaround.

- CSCub84708

  The value for the "Total activated EPS Idle Sessions" counter in the **show gprs gtp status** command output is much higher than the value for the "Total activated sessions" counter.

  The "Total activated EPS Idle Sessions" counter is incorrectly incremented or decremented when the following conditions occur:

  - A handoff cancellation.
  - DSR after an initial attach.
  - Handover request came in without data path info.

  Workaround: There is currently no known workaround.

- CSCuc02585

  The gateway crashes when flooded with Modify Bearer Requests.

  This condition occurs during continuous S4-to-S11 handoffs with mobility rate of 1200 when charging DRTs get rejected. Rejected DRTs leads to the accumulation of CDRs, and the memory occupied by the CDRs grows more than the limit, which results in the gateway crashing.

  Workaround: There is currently no known workaround.

- CSCuc11009

  The Cisco LTE SPGW crashes at "adj_switch_ipv4_generic_les" when processing downlink data packets.

  This condition occurs because of some inappropriate length in packet/calculations.

  Workaround: There is currently no known workaround.

- CSCuc30164

  The active Cisco LTE SPGW reloads with rate_limit_loop traceback. This condition occurs on the active SPGW during handovers with high data rates.

  Workaround: There is currently no known workaround.

- CSCuc84209

  The following syslog and traceback is seen on the active Cisco LTE SPGW:

```
SAMI 1/8: 000352: Oct 17 16:30:46: %GTP-7-GWDEBUG: PDP:0x065D100C, refcnt:0, Wrong
refcnt when charging_reserved,  -Traceback= 0x834586Cz 0x82C7004z 0x8054194z
0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000353: Oct 17 16:31:29: %ALIGN-3-SPURIOUS: Spurious memory access made at
0x82C5EC0z  reading 0xD4
SAMI 1/8: 000354: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C5EC0z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000355: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x8304178z 0x82C5F18z
0x82C6FE8z 0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz
SAMI 1/8: 000356: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C60A8z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000357: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C6150z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000358: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x83456F0z 0x82C7004z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
```

The syslog and traceback is seen on active SPGW during the execution of the **show gprs gtp pdp-context tid all** command.

Workaround: There is currently no known workaround.

- CSCuc95775

  A crash is observed when deleting sessions.

  This condition occurs when DSR is sent with more calls per second (CPS) for approximately 150k sessions.

  Workaround: There is currently no known workaround.

- CSCud04444

  The Cisco LTE SPGW crashes with an unexpected exception to CPU.

  This condition is seen with an accounting feature after a prolonged stress test.

  Workaround: There is currently no known workaround.

- CSCud04466

  The Cisco LTE SPGW crashes due to an unexpected exception to CPU.

  This condition occurs with the Cisco IOS Cisco Express Forwarding (CEF) feature after prolonged stress conditions.

  Workaround: There is currently no known workaround.

- CSCud05773

  The Cisco LTE SPGW crashes with an Unexpected exception to CPU.

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCud24362

  A memory crash is seen while doing create/delete call-model tests with over 2.4 million UEs.

  Workaround: There is currently no known workaround.

- CSCud34267

  A crash occurs “@pak_has_particles (0x99eab9c)+0x4” during a 2.4M call model run.

  Workaround: There is currently no known workaround.

- CSCud09932

  The Cisco LTE SPGW crashes with “CPU exception.”

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCue20819

  Memory leaks are observed on the gateway under certain conditions.

  A PGW data Finite State Machine (FSM) leak is seen when there is a GTPv1 SP or P-SP handoff without establishing the data path. A GPRS list elem leak is seen when a create PDP fails on the standby gateway because of a resource issue.

  Workaround: There is currently no known workaround.

- CSCuf00649

The Cisco LTE SPGW crashes.

While processing the SCU message from the Cisco CSG2, if the SPGW has an invalid PDP in the mcb structure, the gateway crashes.

Workaround: There is currently no known workaround.

- CSCuf76872

  The Cisco LTE SPGW fails to delete a Lawful Intercept (LI) SS8 Mediation Device (MD) entry. Therefore, the MD is unable to provision any LI TAPs.

  This condition occurs because of a stale mobility stream entry. This can occur when two MDs (SS8) are used to set multiple user taps for the same users.

  Workaround: Use just one SS8 MD for LI provisioning. If the issue has already occurred on an SPGW, manually reload both the active and standby gateway together at the same time.

- CSCuf00799

  A Cisco LTE SPGW crash occurs with an accounting session ID traceback.

  This condition occurs when a stale session is present in the standby for the same transaction identifier (TID).

  Workaround: Reload the standby.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4m.

- 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 occasion 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.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

  Workaround: There is currently no known workaround.

- CSCua36249

  When an Xscale CPU reload occurs because of a QNX crash, the Cisco SAMI network processor (IXP) console displays the reload reason as UNKNOWN (IXP CAUSE = NP Core Reset - Cause Unknown).

  This condition occurs when there is a QNX microkernel crash on the Xscale CPU.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4l. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 49
- Cisco SAMI Resolved Caveats, page 49

Cisco LTE SPGW Resolved Caveats

There are no newly resolved SPGW-specific caveats in Cisco IOS Release 12.4(24)T4m.

Cisco SAMI Resolved Caveats

The following Cisco SAMI caveat is resolved with Cisco IOS Release 12.4(24)T4m.

- CSCue20323

  The uplink traffic from an UE is unable to reach the Internet because the SPGW does not forward the same data.

  This condition is seen when QM drops in the Cisco SAMI IXP are occurring.

Caveats - Cisco IOS Release 12.4(24)T4l

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1j, Cisco IOS Release 12.4(24)T4l image:

- Open Caveats, page 49
- Resolved Caveats, page 53

Open Caveats

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

- Cisco LTE SPGW Open Caveats, page 49
- Cisco SAMI Open Caveats, page 52

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4l.

- CSCtf14093

  Network Management System (NMS) poll on CISCO-IP-LOCAL-POOL-MIB does not provide IPv6 local pool entries.

  This condition is seen when an SNMP poll is done on CISCO-IP-LOCAL-POOL-MIB from Mobile Wireless Transport Manager (MWTM) or any other NMS. As a result of this condition, monitoring IPv6 local pools via an NMS not possible.

  Workaround: There is currently no known workaround.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCtz55440

  The QCI status counters that display in the **show gprs qos status** command output do not increment on the standby gateway after a session is deleted.

  This condition occurs with an active-standby gateway configuration when a PDP is created and the same PDP is deleted on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCub25920

  Some of the handover counters do not increment properly in the **show gprs gtp statistics** command output.

  This condition occurs with the following counters:

  - P to SP change
    failed 0
  - P to GGSN change
    success 0
  - SP to GGSN change
    success 0
  - GGSN to SP change
    failed 0

  Workaround: There is currently no known workaround.

- CSCub84708

  The value for the "Total activated EPS Idle Sessions" counter in the **show gprs gtp status** command output is much higher than the value for the "Total activated sessions" counter.

  The "Total activated EPS Idle Sessions" counter is incorrectly incremented or decremented when the following conditions occur:

- A handoff cancellation.
- DSR after an initial attach.
- Handover request came in without data path info.

Workaround: There is currently no known workaround.

- CSCuc02585

  The gateway crashes when flooded with Modify Bearer Requests.

  This condition occurs during continuous S4-to-S11 handoffs with mobility rate of 1200 when charging DRTs get rejected. Rejected DRTs leads to the accumulation of CDRs, and the memory occupied by the CDRs grows more than the limit, which results in the gateway crashing.

  Workaround: There is currently no known workaround.

- CSCuc11009

  The Cisco LTE SPGW crashes at “adj_switch_ipv4_generic_les” when processing downlink data packets.

  This condition occurs because of some inappropriate length in packet/calculations.

  Workaround: There is currently no known workaround.

- CSCuc30164

  The active Cisco LTE SPGW reloads with rate_limit_loop traceback. This condition occurs on the active SPGW during handovers with high data rates.

  Workaround: There is currently no known workaround.

- CSCuc84209

  The following syslog and traceback is seen on the active Cisco LTE SPGW:

  ```
  SAMI 1/8: 000352: Oct 17 16:30:46: %GTP-7-GWDEBUG: PDP:0x065D100C, refcnt:0, Wrong
  refcnt when charging_reserved,  -Traceback= 0x834586Cz 0x82C7004z 0x8054194z
  0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000353: Oct 17 16:31:29: %ALIGN-3-SPURIOUS: Spurious memory access made at
  0x82C5EC0z  reading 0xD4
  SAMI 1/8: 000354: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C5EC0z 0x82C6FE8z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000355: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x8304178z 0x82C5F18z
  0x82C6FE8z 0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz
  SAMI 1/8: 000356: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C60A8z 0x82C6FE8z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000357: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C6150z 0x82C6FE8z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000358: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x83456F0z 0x82C7004z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  ```

  The syslog and traceback is seen on active SPGW during the execution of the **show gprs gtp pdp-context tid all** command.

  Workaround: There is currently no known workaround.

- CSCuc95775

  A crash is observed when deleting sessions.

  This condition occurs when DSR is sent with more calls per second (CPS) for approximately 150k sessions.

  Workaround: There is currently no known workaround.

- CSCud04444

The Cisco LTE SPGW crashes with an unexpected exception to CPU.

This condition is seen with an accounting feature after a prolonged stress test.

Workaround: There is currently no known workaround.

- CSCud04466

  The Cisco LTE SPGW crashes due to an unexpected exception to CPU.

  This condition occurs with the Cisco IOS Cisco Express Forwarding (CEF) feature after prolonged stress conditions.

  Workaround: There is currently no known workaround.

- CSCud05773

  The Cisco LTE SPGW crashes with an Unexpected exception to CPU.

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCud24362

  A memory crash is seen while doing create/delete call-model tests with over 2.4 million UEs.

  Workaround: There is currently no known workaround.

- CSCud34267

  A crash occurs "@pak_has_particles (0x99eab9c)+0x4" during a 2.4M call model run.

  Workaround: There is currently no known workaround.

- CSCud09932

  The Cisco LTE SPGW crashes with "CPU exception."

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCue20819

  Memory leaks are observed on the gateway under certain conditions.

  A PGW data Finite State Machine (FSM) leak is seen when there is a GTPv1 SP or P-SP handoff without establishing the data path. A GPRS list elem leak is seen when a create PDP fails on the standby gateway because of a resource issue.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4l.

- 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 occasion 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.

- CSCtx85422

One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

Workaround: There is currently no known workaround.

- CSCua36249

  When an Xscale CPU reload occurs because of a QNX crash, the Cisco SAMI network processor (IXP) console displays the reload reason as UNKNOWN (IXP CAUSE = NP Core Reset - Cause Unknown).

  This condition occurs when there is a QNX microkernel crash on the Xscale CPU.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4m. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 53
- Cisco SAMI Resolved Caveats, page 53

Cisco LTE SPGW Resolved Caveats

There are no newly resolved SPGW-specific caveats in Cisco IOS Release 12.4(24)Tl.

Cisco SAMI Resolved Caveats

The following Cisco SAMI caveats are resolved with Cisco IOS Release 12.4(24)T4l.

- CSCuc65113

  A LCP system manager crash occurs due to the corruption of processor memory information.

  When this condition occurs, the core dump file contains the processor memory information details.

- CSCud47702

  The Cisco SAMI LCP produces the following logs:

  ```
  %SAMI-3-730205: SAMI User Space: ERROR: IXP xscale core rcvd. 1 collect crashinfo
  ```

  The ixp1_crash.txt has this entry:

  ```
  IXP CAUSE = NP Watchdog Reset
  ```

  The 20121121-201846_crashinfo_collection-20121117-103238.tar contains qnx_1_sysmgr_g_ns_126985_core.

- CSCue48009

  QM1 drops a lot of packets due to SPI-4 flow control incrementing to a large number, which inserts back pressure to the IXP. A Tx1 is processing a packet whose metadata contains an invalid large packet length in the range of 0xffde.

This condition of dumping q-arrays in the SRAM channel 0 at 0x1000 location from the Rx ME on receiving Drop All packet signs from the Lookup and Queue Manager ME occurs with the following conditions.

- QM0_INVALID_PACKET_LENGTH
- QM0_INPUT_NULL_BUFFER_HANDLE
- QM0_OUTPUT_NULL_BUFFER_HANDLE
- QM1_INVALID_PACKET_LENGTH
- QM1_INPUT_NULL_BUFFER_HANDLE
- QM1_OUTPUT_NULL_BUFFER_HANDLE
- LOOKUP_LM_RX_INFO_INVALID

- CSCue48044

  A browsing issue is seen on some of test UEs.

  When this condition occurs, some SPI-4 flow control counters are incrementing in large number and QM1 drops are occurring at the same time.

```
SPGWA#show sami ixp statistics de | i SPI
[RX0] SPI4 Length Error = 0
[RX0] SPI4 Parity Error = 0
[RX0] SPI4 Aborts = 0
[TX0] SPI-4 flow control = 0
[TX1] SPI-4 flow control = 4181321618
[RX0] SPI4 Length Error = 0
[RX0] SPI4 Parity Error = 0
[RX0] SPI4 Aborts = 0
[TX0] SPI-4 flow control = 0
[TX1] SPI-4 flow control = 1263087613
SPGWA#sh sami ixp statistics de | i Dropped
[RESEQ0] Dropped = 131355
[QM0] Dropped = 0
[QM1] Dropped = 79365710
[RESEQ0] Dropped = 124093
[QM0] Dropped = 0
[QM1] Dropped = 81003021
```

  This condition occurs when Tx1 is processing a packet in which the metadata contains an invalid long length in the range of 0xffde.

Caveats - Cisco IOS Release 12.4(24)T4k

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1h, Cisco IOS Release 12.4(24)T4k image:

- Open Caveats, page 54
- Resolved Caveats, page 58

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 59
- Cisco SAMI Open Caveats, page 62

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4k.

- CSCtf14093

  Network Management System (NMS) poll on CISCO-IP-LOCAL-POOL-MIB does not provide IPv6 local pool entries.

  This condition is seen when an SNMP poll is done on CISCO-IP-LOCAL-POOL-MIB from Mobile Wireless Transport Manager (MWTM) or any other NMS. As a result of this condition, monitoring IPv6 local pools via an NMS not possible.

  Workaround: There is currently no known workaround.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCtz55440

  The QCI status counters that display in the **show gprs qos status** command output do not increment on the standby gateway after a session is deleted.

  This condition occurs with an active-standby gateway configuration when a PDP is created and the same PDP is deleted on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCub25920

  Some of the handover counters do not increment properly in the **show gprs gtp statistics** command output.

This condition occurs with the following counters:

- P to SP change
  failed 0
- P to GGSN change
  success 0
- SP to GGSN change
  success 0
- GGSN to SP change
  failed 0

Workaround: There is currently no known workaround.

- CSCub84708

  The value for the "Total activated EPS Idle Sessions" counter in the **show gprs gtp status** command output is much higher than the value for the "Total activated sessions" counter.

  The "Total activated EPS Idle Sessions" counter is incorrectly incremented or decremented when the following conditions occur:

  - A handoff cancellation.
  - DSR after an initial attach.
  - Handover request came in without data path info.

  Workaround: There is currently no known workaround.

- CSCuc02585

  The gateway crashes when flooded with Modify Bearer Requests.

  This condition occurs during continuous S4-to-S11 handoffs with mobility rate of 1200 when charging DRTs get rejected. Rejected DRTs leads to the accumulation of CDRs, and the memory occupied by the CDRs grows more than the limit, which results in the gateway crashing.

  Workaround: There is currently no known workaround.

- CSCuc11009

  The Cisco LTE SPGW crashes at "adj_switch_ipv4_generic_les" when processing downlink data packets.

  This condition occurs because of some inappropriate length in packet/calculations.

  Workaround: There is currently no known workaround.

- CSCuc30164

  The active Cisco LTE SPGW reloads with rate_limit_loop traceback. This condition occurs on the active SPGW during handovers with high data rates.

  Workaround: There is currently no known workaround.

- CSCuc84209

  The following syslog and traceback is seen on the active Cisco LTE SPGW:

```
SAMI 1/8: 000352: Oct 17 16:30:46: %GTP-7-GWDEBUG: PDP:0x065D100C, refcnt:0, Wrong
refcnt when charging_reserved,  -Traceback= 0x834586Cz 0x82C7004z 0x8054194z
0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000353: Oct 17 16:31:29: %ALIGN-3-SPURIOUS: Spurious memory access made at
0x82C5EC0z  reading 0xD4
SAMI 1/8: 000354: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C5EC0z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
```

```
SAMI 1/8: 000355: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x8304178z 0x82C5F18z
0x82C6FE8z 0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz
SAMI 1/8: 000356: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C60A8z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000357: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C6150z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000358: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x83456F0z 0x82C7004z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
```

The syslog and traceback is seen on active SPGW during the execution of the **show gprs gtp pdp-context tid all** command.

Workaround: There is currently no known workaround.

- CSCuc95775

  A crash is observed when deleting sessions.

  This condition occurs when DSR is sent with more calls per second (CPS) for approximately 150k sessions.

  Workaround: There is currently no known workaround.

- CSCud04444

  The Cisco LTE SPGW crashes with an unexpected exception to CPU.

  This condition is seen with an accounting feature after a prolonged stress test.

  Workaround: There is currently no known workaround.

- CSCud04466

  The Cisco LTE SPGW crashes due to an unexpected exception to CPU.

  This condition occurs with the Cisco IOS Cisco Express Forwarding (CEF) feature after prolonged stress conditions.

  Workaround: There is currently no known workaround.

- CSCud05773

  The Cisco LTE SPGW crashes with an Unexpected exception to CPU.

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCud24362

  A memory crash is seen while doing create/delete call-model tests with over 2.4 million UEs.

  Workaround: There is currently no known workaround.

- CSCud34267

  A crash occurs “@pak_has_particles (0x99eab9c)+0x4” during a 2.4M call model run.

  Workaround: There is currently no known workaround.

- CSCud09932

  The Cisco LTE SPGW crashes with “CPU exception.”

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCue20819

  Memory leaks are observed on the gateway under certain conditions.

A PGW data Finite State Machine (FSM) leak is seen when there is a GTPv1 SP or P-SP handoff without establishing the data path. A GPRS list elem leak is seen when a create PDP fails on the standby gateway because of a resource issue.

Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4k.

- 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 occasion 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.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

  Workaround: There is currently no known workaround.

- CSCua36249

  When an Xscale CPU reload occurs because of a QNX crash, the Cisco SAMI network processor (IXP) console displays the reload reason as UNKNOWN (IXP CAUSE = NP Core Reset - Cause Unknown).

  This condition occurs when there is a QNX microkernel crash on the Xscale CPU.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4k. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 58
- Cisco SAMI Resolved Caveats, page 59

Cisco LTE SPGW Resolved Caveats

This section lists SPGW-specific caveats that are resolved in Cisco IOS Release 12.4(24)T4k.

- CSCue01948

  An IO memory leak is observed on the gateway in addition to a processor memory leak.

This condition occurs when the Mobile Management Entity (MME) sends a Downlink Data Notification (DDN) Ack with a “Context Not Found” cause. When the MME sends a DDN Ack with a “Context Not Found” cause, the gateway does not to the Finite State Machine (FSM) cleanup, which leads to a IO memory leak, as well as an processor memory leak.

- CSCud97951

  Memory chunk leaks are seen on the gateway. Specifically, the memory chunk leaks occur with PCP and MCB structures.

  This condition occurs when there is an Update PDP Context Request for GTPv2-toGTPv1 handoff or for an inter Gn/Gp SGSN handoff for a PDP and the update is synchronized to the standby gateway.

  The memory chunk leaks are seen on the standby gateway after the PDP is deleted.

Cisco SAMI Resolved Caveats

The are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)T4k.

Caveats - Cisco IOS Release 12.4(24)T4j

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1i, Cisco IOS Release 12.4(24)T4j image:

- Open Caveats, page 59
- Resolved Caveats, page 63

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 59
- Cisco SAMI Open Caveats, page 62

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4j.

- CSCtf14093

  Network Management System (NMS) poll on CISCO-IP-LOCAL-POOL-MIB does not provide IPv6 local pool entries.

  This condition is seen when an SNMP poll is done on CISCO-IP-LOCAL-POOL-MIB from Mobile Wireless Transport Manager (MWTM) or any other NMS. As a result of this condition, monitoring IPv6 local pools via an NMS not possible.

  Workaround: There is currently no known workaround.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCtz55440

  The QCI status counters that display in the **show gprs qos status** command output do not increment on the standby gateway after a session is deleted.

  This condition occurs with an active-standby gateway configuration when a PDP is created and the same PDP is deleted on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCub25920

  Some of the handover counters do not increment properly in the **show gprs gtp statistics** command output.

  This condition occurs with the following counters:

  - P to SP change
    failed 0
  - P to GGSN change
    success 0
  - SP to GGSN change
    success 0
  - GGSN to SP change
    failed 0

  Workaround: There is currently no known workaround.

- CSCub84708

  The value for the "Total activated EPS Idle Sessions" counter in the **show gprs gtp status** command output is much higher than the value for the "Total activated sessions" counter.

  The "Total activated EPS Idle Sessions" counter is incorrectly incremented or decremented when the following conditions occur:

- A handoff cancellation.
- DSR after an initial attach.
- Handover request came in without data path info.

Workaround: There is currently no known workaround.

- CSCuc02585

  The gateway crashes when flooded with Modify Bearer Requests.

  This condition occurs during continuous S4-to-S11 handoffs with mobility rate of 1200 when charging DRTs get rejected. Rejected DRTs leads to the accumulation of CDRs, and the memory occupied by the CDRs grows more than the limit, which results in the gateway crashing.

  Workaround: There is currently no known workaround.

- CSCuc11009

  The Cisco LTE SPGW crashes at “adj_switch_ipv4_generic_les” when processing downlink data packets.

  This condition occurs because of some inappropriate length in packet/calculations.

  Workaround: There is currently no known workaround.

- CSCuc30164

  The active Cisco LTE SPGW reloads with rate_limit_loop traceback. This condition occurs on the active SPGW during handovers with high data rates.

  Workaround: There is currently no known workaround.

- CSCuc84209

  The following syslog and traceback is seen on the active Cisco LTE SPGW:

  ```
  SAMI 1/8: 000352: Oct 17 16:30:46: %GTP-7-GWDEBUG: PDP:0x065D100C, refcnt:0, Wrong
  refcnt when charging_reserved,  -Traceback= 0x834586Cz 0x82C7004z 0x8054194z
  0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000353: Oct 17 16:31:29: %ALIGN-3-SPURIOUS: Spurious memory access made at
  0x82C5EC0z  reading 0xD4
  SAMI 1/8: 000354: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C5EC0z 0x82C6FE8z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000355: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x8304178z 0x82C5F18z
  0x82C6FE8z 0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz
  SAMI 1/8: 000356: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C60A8z 0x82C6FE8z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000357: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C6150z 0x82C6FE8z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  SAMI 1/8: 000358: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x83456F0z 0x82C7004z
  0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
  ```

  The syslog and traceback is seen on active SPGW during the execution of the **show gprs gtp pdp-context tid all** command.

  Workaround: There is currently no known workaround.

- CSCuc95775

  A crash is observed when deleting sessions.

  This condition occurs when DSR is sent with more calls per second (CPS) for approximately 150k sessions.

  Workaround: There is currently no known workaround.

- CSCud04444

The Cisco LTE SPGW crashes with an unexpected exception to CPU.

This condition is seen with an accounting feature after a prolonged stress test.

Workaround: There is currently no known workaround.

- CSCud04466

  The Cisco LTE SPGW crashes due to an unexpected exception to CPU.

  This condition occurs with the Cisco IOS Cisco Express Forwarding (CEF) feature after prolonged stress conditions.

  Workaround: There is currently no known workaround.

- CSCud05773

  The Cisco LTE SPGW crashes with an Unexpected exception to CPU.

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCud24362

  A memory crash is seen while doing create/delete call-model tests with over 2.4 million UEs.

  Workaround: There is currently no known workaround.

- CSCud34267

  A crash occurs "@pak_has_particles (0x99eab9c)+0x4" during a 2.4M call model run.

  Workaround: There is currently no known workaround.

- CSCud09932

  The Cisco LTE SPGW crashes with "CPU exception."

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4j.

- 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 occasion 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.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

  Workaround: There is currently no known workaround.

- CSCua36249

  When an Xscale CPU reload occurs because of a QNX crash, the Cisco SAMI network processor (IXP) console displays the reload reason as UNKNOWN (IXP CAUSE = NP Core Reset - Cause Unknown).

  This condition occurs when there is a QNX microkernel crash on the Xscale CPU.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4i. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 63
- Cisco SAMI Resolved Caveats, page 69

Cisco LTE SPGW Resolved Caveats

This section lists SPGW-specific caveats that are resolved in Cisco IOS Release 12.4(24)T4j.

- CSCtx91844

  The "S1/X2 change counter" does not increment in the **show gprs gtp statistics** command output after a handover.

  This condition is seen with the following scenario:

  a. S1 with no SGW change.
  b. S1 with an SGW change.
  c. X2 with no SGW change.
  d. X2 with an SGW change.

  Additionally, the S1 and X2 counters are calculated incorrectly; therefore, they are not serving the purpose for which they are intended. The S1 and X2 counters generate incorrect information while debugging as well.

- CSCtx93599

  The Cisco LTE SPGW closes a P-CDR with a value of 24 before a switchover or with a value of 18 after a switchover during a PGW-to-SPGW mode change as part of an S1-base handover.

  This condition happens on the newly active gateway if an SPGW switchover occurs before a final modify bearer request comes to the SPGW to complete the S1-based handover.

- CSCty03462

  The Cisco LTE SPGW detects a Public Land Mobile Network (PLMN) change during a 3G-to-4G or 4G-to-3G handoff, and sets the PLMN ID change bit in the change condition for the service container.

  This condition occurs with an inter-routing access technology handoff.

- CSCty76309

  The following error message displays in the gateway:

  ```
  %ADJ-3-ADJSTACK2: Adj stack2 error IPV6 midchain out of Virtual-Access5, addr
  2606:AE:C05D:7B2::C8 (incomplete): cannot stack on linktype requested: gtp tunnel st:
  ```

This message displays with 100k IPv6 users and continuous IPv6 traffic with failover in between. The error message occurs during the switchover.

- CSCtz09158

  The following counters are not incremented in the show gprs gtp statistics command output:

  Message Statistics:

Rcvd PDU msg	0	Sent PDU msg	0
Rcvd PDU bytes	0	Sent PDU bytes	0

  This condition occurs when Mobile Express Forwarding (MEF) is enabled.

- CSCtz98897

  When deleting a partially created PDP, the Stop Indicator is not present in the Accounting Stop. Therefore, the Policy and Charging Enforcement Function (PCEF) (Cisco CSG2) fails to remove the known user table (KUT) entry.

  This condition occurs when a new create request is received from the from Mobility Management Entity (MME) for an existing PDP session that is not created. With this scenario, the partially created PDP session is deleted to address the new create request from the MME.

- CSCua14402

  A handover request with a new path restart counter fails, but the path is restarted and the existing PDPs on the path are deleted.

  This condition occurs when a handover request to an existing path with new restart counter is dropped by the gateway.

- CSCua92415

  The gateway crashes when the TCP link of the charging gateway goes down or flaps.

  This condition occurs when the path protocol configured is TCP and link up/down events occur, which trigger open and close socket events on a Cisco SAMI PowerPC (PPC), which also learns the link state information from other PPCs at the same time.

- CSCua92426

  The standby Proxy Control Processor (PCOP) moves to STANDBY HOT before all of the Traffic and Control Plane processors (TCOPs).

  This condition occurs when the standby gateway comes up.

- CSCub25231

  The Aggregate Maximum Bit Rate (AMBR) is included in the Create PDP Response when it is not requested by the SGSN.

  This condition occurs when a create PDP context request does not contain an AMBR information element (IE).

- CSCub83636

  The following spurious memory access and bad ID syslog is seen:

```
2855309: SAMI 1/5: 000036: Aug 21 10:17:28: %IDMGR-3-INVALID_ID: bad id in id_to_ptr
(bad id) (id: 0x0),  -Traceback= 0xA2A3F58z 0x828D7D4z 0x9E914C8z 0x9E91730z
0x9E72E00z 0x9E75B68z 0xA2927F4z 0xA2928A4z 0x9E90670z 0x9E92954z 0x9E6FFC8z
0x9EB5ECCz 0x8297CCCz 0x828FA30z 0x8290424z 0x99D2BECz

2855310: SAMI 1/5: 000037: Aug 21 10:17:35: %ALIGN-3-SPURIOUS: Spurious memory access
made at 0x828D7CCz  reading 0x2EC
```

```
2855311: SAMI 1/5: 000038: Aug 21 10:17:35: %ALIGN-3-TRACE: -Traceback= 0x828D7CCz
0x9E914C8z 0x9E91730z 0x9E72E00z 0x9E75B68z 0xA2927F4z 0xA2928A4z 0x9E90670z
```

This condition occurs when the policy charging rules function (PCRF) sends a Dedicated Bearer Creation Request to the gateway.

- CSCub95135

  The following syslog with traceback is seen:

  ```
  SAMI 2/6: 000111: May  8 11:19:04.505 EDT:  %GPRSFLTMG-3-GPRS_UNEXPECTED_EVENT:
  Unexpected condition: Attempting to free PDP without deleting accounting hash node,
  -Traceback= 0x8332A2Cz 0x8333C24z 0x80528F0z 0x80530F8z 0x9DB49D4z 0x9EA25B0z
  0x9EA2604z 0x9DC54C8z 0x9E2B8F8z 0x9E2DFE0z 0xA28FD78z 0xA28FDE8z 0x9E2629Cz
  0x9E26C74z 0x9E54D20z 0x9E5FC2Cz
  ```

  This condition occurs when the gateway is waiting for an IXP response and an accounting response, or COA is received instead, which causes the session to be deleted and the traceback to occur.

- CSCuc11119

  Spurious memory access is seen while freeing buffer to memory.

  This condition occurs when downlink packets are sent, the data path is blocked, buffering is enabled, and the eNode-b link type is IPv6.

- CSCuc13861

  The gateway might crash with an “SCTP out of Window” message displayed on the console.

  This condition occurs during the re-assembly of data chunks and the transmission sequence number (TSN) of the chunk wrapped and became 0 (zero). The re-assembly logic failed and falsely indicated a gap in the message and the application was not signaled to read the message.

  Because of this, recv window was exhausted, resulting in the “SCTP out of window” message.

- CSCuc15645

  The standby gateway crashed while trying to send a modify PDP request to the Cisco SAMI IXP. The crash occurs because the PDP is already deleted, and therefore, it is invalid. Accessing this invalid memory causes the crash.

  This condition occurs when a Modify PDP occurs in two scenarios on the standby gateway: 1) during the standby synchronization and 2) when the path is updated.

  As a result, with a modify PDP a “blocking call” occurs to create QoS rate profiles (two rate profiles: one for downlink QoS and the other for uplink QoS on the IXP). “Blocking call” means that the process suspends so each update waits at one call and when the first blocking call finishes, it executes the standby delete event for the PDP and deletes the PDP. When the second blocked call is completed, it attempts to access PDP memory, which cause the gateway to crash because the PDP is no longer valid.

- CSCuc30748

  The following syslog displays in the gateway:

  ```
  SAMI 11/3: Sep 21 16:20:22.954: %IPC-3-SAMI_SM_FAIL_DUP_MSISDN: Unexpected condition:
  TCOP in IMSI-Sticky doesn't match withMSISDN-Sticky MSISDN: 3DUf IMSI 804433445566110
  ```

  In a 3G-to-4G handoff scenario in which there is a CSReq without a mobile station ISDN (MSISDN) Informational Element (IE), when the same user moves to another Traffic and Control Plane processor (TCOP), the syslog displays.

- CSCuc38645

A Modify Bearer Request (MBR) without an S5/S8 Tunnel Endpoint ID (TEID) is incorrectly processed as a handoff.

This condition occurs with the following scenarios:

- Case1: MBR is rejected because of incorrect mandatory IE. This MBR is an invalid or old MBR delayed for some reason, which reaches the gateway after the PDP moved to GGSN-mode. When the PDP is in GGSN-mode, and an MBR without an SGW S5/S8 Fully Qualified Tunnel End Point Identifier (FTEID) is received, the system assumes this to be a GGSN-to-P handoff request and attempts to check for APN AMBR. It rejects the PDP because the perceived mandatory IE (APN AMBR) is missing.
- Case2: During a P-to-SP handoff, when the PDP is in SPGW [HO] mode and the gateway wrongly receives an MBR from an old pat, the handoff is completed with the assumption the MBR is from a new path.

- CSCuc38677

  The counters for the Echo statistics display a higher number in the Echo Responses Send counter than the number of Echo Requests Received.

  This condition occurs if the Echo Request is in cache. If the Echo Request is in cache, then the Echo Response Send counter is incremented but not Echo Request Received counter.

- CSCuc41495 (duplicate of CSCuc50097)

  The CSReq for SGW relocation is rejected with an incorrect mandatory information element.

  This condition occurs when the gateway already has a session in PGW-, GGSN-, or SPGW-mode with the same IMSI + EBI values, but the new CSR came for creating SGW portion. This issue will occur if there is a stale PDP on the gateway.

- CSCuc50097

  When attempting to create a GGSN/PGW-mode session over an SGW mode session, the create over create fails.

  This condition occurs with a create GGSN/ PGW-mode over create SGW-mode, because the gateway checks for GTPv1/GTPv0 PDP and then the gateway deletes and recreates in PGW-mode, which causes the create to fail.

- CSCuc56883

  The following syslog is seen “Syslog seen %GTPSR-6-GTPSBYPDPSTATE: GTP-SR: PDP check: Type:1, Evt:GW_SR_EVENT_DEL_SESS_REQ_HANDOVER.”

  This syslog is seen in the standby gateway under certain scenarios when the gateway is in [HO] state for the PDP and the PDP is deleted.

- CSCuc58401

  The gateway CDR MSTimezone trigger does not reset the current volume or time triggers for the UE.

  This condition occurs only when MEF traffic switching is used for the session.

- CSCuc80126

  The following spurious memory access is seen while handling a Downlink Data Notification (DDN):

  ```
  451748: SAMI 3/5: 006717: Oct 18 11:07:43: %ALIGN-3-SPURIOUS: Spurious memory access
  made at 0x9EA7A50z  reading 0x2
  451749: SAMI 3/5: 006718: Oct 18 11:07:43: %ALIGN-3-TRACE: -Traceback= 0x9EA7A50z
  0x97B8E10z 0x97B8F40z 0x9E5D770z 0x83145E4z 0x99D792Cz 0x99DB0B4z 0x0z
  ```

  Spurious memory access is made while trying to read the saved DDN packet in the T3 Timer handler.

- CSCuc83309

  High CPU usage is seen in the gateway when packets that are denied in an access list are process switched.

- CSCuc84183

  The following traceback is seen:

```
SAMI 4/8: 006605: Oct 23 12:03:33: %ALIGN-3-SPURIOUS: Spurious memory access made at
0x9E9A644z  reading 0x4
SAMI 4/8: 006606: Oct 23 12:03:33: %ALIGN-3-TRACE: -Traceback= 0x9E9A644z 0x9E9A5ECz
0x9EA42F0z 0x9EB0760z 0x83145B4z 0x99D792Cz 0x99DB0B4z 0x0z
SAMI 4/8: 006607: Oct 23 12:03:33: %ALIGN-3-TRACE: -Traceback= 0x9E9A648z 0x9E9A5ECz
0x9EA42F0z 0x9EB0760z 0x83145B4z 0x99D792Cz 0x99DB0B4z 0x0z
SAMI 4/8: 006608: Oct 23 12:03:33: %ALIGN-3-TRACE: -Traceback= 0x9EA7A50z 0x97B8E10z
0x97B8F40z 0x9E5D770z 0x83145E4z 0x99D792Cz 0x99DB0B4z 0x0z
```

  This traceback is seen while processing Downlink Data Notification (DDN) Ack message during a Gtpv2 iRAT handover.

- CSCuc84491

  The following syslog is seen:

```
SAMI 1/7: 006401: Oct 23 15:23:35: %SYS-2-BADSHARE: Bad refcount in pak_enqueue,
ptr=209F3BB8,
count=0,  -Traceback= 0x997BC94z 0x997D914z 0x8321C5Cz 0x9DE3660z 0x9E9FEC4z
0x9EA4074z 0x9EB0760z
0x83145B4z 0x99D792Cz 0x99DB0B4z
SAMI 1/7: 006402: Oct 23 15:23:35: %SYS-2-BADSHARE: Bad refcount in datagram_done,
ptr=209F3BB8,
count=0,  -Traceback= 0x9976888z 0x997DB04z 0x8321C5Cz 0x9DE3660z 0x9E9FEC4z
0x9EA4074z 0x9EB0760z
0x83145B4z 0x99D792Cz 0x99DB0B4z
```

  This syslog is seen when there are more than 16 messages (or events) for a PDP to be processed. Because of this, the wait queue is full and when the gateway tries to send a negative response, it displays this syslog.

- CSCuc88363

  An Modify Bearer Request (MBR) for a GTPv1-to-SP handoff fails with an incorrect mandatory information element (IE). During the GTPv1-to-SP handoff, the sender Fully Qualified Tunnel End Point Identifier (FTEID) is present in the MBR request.

- CSCuc90802

  The following syslog is seen during the deletion of a PDP when the update PDP synchronization on the standby gateway failed because of a sync decode failure:

  GTP-7-GTPPDPSTATE: GTP: PDP check:

- CSCuc98212

  The Cisco LTE SPGW crashes due to an unexpected exception to CPU.

  This condition occurs when an MBR for a GTPv1-to-GTPv2 handoff with “Bearer Context to be removed” in the message is received.

- CSCud00199

  A valid Modify Bearer Request (MBR) for SP-to-PGW mode handoff is rejected.

  This condition occurs during an SP-to-PGW mode handoff when the MBR is sent with an S5/S8 Fully Qualified Tunnel End Point Identifier (FTEID). The Cisco gateway rejects the request with mandatory information element (IE) incorrect.

- CSCud03594

  Call detail records (CDRs) show the PLMN as 000.

  This condition occurs when the UE is created with a Tracking Area in the Create Session Request (CSR) or Modify Bearer Request (MBR). The CDRs show the PLMN as 000. When the UE is created with an S4-SGSN and the CSR received with ULI as SAI, then CDRs are sent with the PLMN as zero.

- CSCud05300

  When an N3T3 timeout occurs for a Downlink Data Notification (DDN) for a user, the Cisco LTE SPGW iterates through all sessions (PDPs) for a user and frees buffered downlink data packets. When this condition occurs, a session with freed PDP data structure is because the SPGW accessed invalid memory.

  This condition occurs when:

  a. The standby gateway encountered an error while deleting a GTPv1 (3G user) session and did not cleanup the session completely.
  b. When the gateway became active, a GTPv2 session was successfully created for the same user.
  c. The downlink data path of the GTPv2 session was removed by an Release Access Bearer Request message from the Mobility Management Entity (MME).
  d. When downlink data packets arrived for the GTPv2 session, the gateway sent out a DDN and buffered data packets.
  e. The MME does not respond to the DDN, and on N3T3 timeout of the DDN, the gateway tried to free up buffered packets for all sessions of the user. At this point, the gateway SPGW also tried to access the GTPv1 session that was not completely deleted earlier, which resulted in a reload.

- CSCud21539

  The gateway sends the local control TEID as zero (0) in the Create Session Response to the MME.

  This condition occurs when a new SGW/SP-mode session is being created on the gateway and the same UE already has another session in GTPv1 or PGW-mode on same SPGW with a different APN and Network Service Access Point Identifier (NSAPI)/EBI.

- CSCud49673

  The following spurious access is seen:

```
12025490: SAMI 3/8: 000047: Nov 30 13:01:34: %ALIGN-3-SPURIOUS: Spurious memory access
made at 0x9EA8DD0z  reading 0x6
12025491: SAMI 3/8: 000048: Nov 30 13:01:34: %ALIGN-3-TRACE: -Traceback= 0x9EA8DD0z
0x9EA9184z 0x9EA9978z 0x9EACA98z 0x9EB9D10z 0x8315DDCz 0x99DC5CCz 0x99DFD54z
12025492: SAMI 3/8: 000049: Nov 30 13:01:34: %ALIGN-3-TRACE: -Traceback= 0x9EA8DF8z
0x9EA9184z 0x9EA9978z 0x9EACA98z 0x9EB9D10z 0x8315DDCz 0x99DC5CCz 0x99DFD54z
```

  This spurious access is seen while the gateway is processing a user level message.

- CSCud60311

  The Cisco LTE SPGW reloads with a specific scenario duringa 4G-to-3G handover.

  This condition occurs with the following:

  a. An SP-mode GTPv2 session exists on the SPGW.
  b. An SGSN sends an Update PDP Context request to handover the session to GTPv1.
  c. During the processing of the handover, the SPGW sends an Accouting-Update to the Cisco CSG2 and waits for the CSG2 to send service usage information.

d. Then, the Mobility Management Entity (MME) sends a Delete Session Request message without the LBI and with the SI bit to delete the S-mode part of the session.

e. The SPGW then receives service usage information from the CSG2.

f. The SPGW attempts to process the Delete Session Request message and reloads due to a software error.

- CSCud61949

  Buffers are rejected due to a low memory limit.

  This condition occurs when I/0 memory is going low.

- CSCud66487

  Free I/O memory drops below 15MB.

  This condition occurs when a Radio Access Bearer (RAB) is received for a PDP that is in a deleting state because the packet is leaked and the memory is not freed.

- CSCud68961

  The Cisco LTE SPGW replies with the Virtual-template IP address as the source-IP for a Create PDP Response or a Create Session Response instead of the SLB-IP.

  This condition occurs after the gateway creates a PDP context and then it receives a retransmitted Create PDP Request or Create Session Request for that PDP. If this condition occurs, the response is sent with the Virtual-template IP address instead of the SLB-IP as the source-IP in the IP header.

Cisco SAMI Resolved Caveats

The following Cisco SAMI caveats are resolved with Cisco IOS Release 12.4(24)T4j.

- CSCtt77928

  A crash occurs while executing “ucdump -L lkup1” on the Cisco SAMI IXP.

  This condition occurs only when “ucdump -L lkup1” is executed on the IXP.

- CSCub45666

  The following message is seen:

  ```
  SAMI 2/5: 000032: Jul 13 20:43:42: %PLATFORM-2-DP_IXP_HM_WARN: Failed to receive
  response from IXP1 in 16 retries, system will reboot if it continues to fail receiving
  response in another 16 retries (i.e. in the next 256 milliseconds.)
  SAMI 2/5: 000033: Jul 13 20:43:43: %PLATFORM-1-DP_HM_FAIL: Failed to receive response
  from IXP1. Check `sami health-monitoring' configuration and see `show sami
  health-monitoring' for more info
  ```

  and the **show sami health monitoring** has 32 consecutive misses, which triggers the reload of the Cisco SAMI.

  ```
  ------------------ show sami health-monitoring ------------------
  IXP1: FAILED
      32/0 Missed/Rcvd consecutive responses
      50/14314449 Missed/Rcvd cumulative responses
      0 Failed to send
  IXP2: ACTIVE
      0/14314453 Missed/Rcvd consecutive responses
      0/14314453 Missed/Rcvd cumulative responses
      0 Failed to send
  ```

- CSCuc81107

The system returned to ROM by an IXP xscale core. The "crashinfo_collection-20121107-154941.tar" contains the qnx process sami_stat_g_ns process core file.

The causes of this condition are unknown because the core file does not contain valid information and the stack trace is corrupted.

- CSCuc94745

  Global Mobile Express Forwarding (MEF) counters are not available to confirm the number of packets destined to Cisco SAMI which has been MEF switched.

  This condition occurs when the Cisco SAMI configuration contains **mef**.

- CSCud33185

  A "sys_lock_sram: timeout waiting for lock" does not display timestamp and the "sami_stat_g_ns process on detecting NULL pointer" exits without displaying a syslog.

  This occurs with an SRAM lock, and any SRAM table update routine that needs to update the SRAM table (like APN). The PDP displays this message every two minutes, once without a timestamp.

- CSCud11551

  Cisco Express Forwarding (CEF) switching occurs of reassembled packets whose MTU size is bigger than the VLAN INGRESS MTU size.

  This condition occurs when fragmented packets are received on the Cisco SAMI IXP, which then punts them to the PPC. The PPC reassembles the packet and sets the REASSEMBLY HINT and sends the packet back to the IXP, which upon finding the packet size bigger than the VLAN INGRESS MTU size, punts it back to the PPC, which does the CEF switching of this packet, increasing the data path of fragmented packets.

Caveats - Cisco IOS Release 12.4(24)T4i

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1f, Cisco IOS Release 12.4(24)T4i image:

- Open Caveats, page 70
- Resolved Caveats, page 77
- Unreproducible Caveat, page 82

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 71
- Cisco SAMI Open Caveats, page 76

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4i.

- CSCtf14093

  Network Management System (NMS) poll on CISCO-IP-LOCAL-POOL-MIB does not provide IPv6 local pool entries.

  This condition is seen when an SNMP poll is done on CISCO-IP-LOCAL-POOL-MIB from Mobile Wireless Transport Manager (MWTM) or any other NMS. As a result of this condition, monitoring IPv6 local pools via an NMS not possible.

  Workaround: There is currently no known workaround.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx91844

  The "S1/X2 change counter" does not increment in the **show gprs gtp statistics** command output after a handover.

  This condition is seen with the following scenario:

  a. S1 with no SGW change.
  b. S1 with an SGW change.
  c. X2 with no SGW change.
  d. X2 with an SGW change.

  Additionally, the S1 and X2 counters are calculated incorrectly; therefore, they are not serving the purpose for which they are intended. The S1 and X2 counters generate incorrect information while debugging as well.

  Workaround: There is currently no known workaround.

- CSCtx93599

  The Cisco LTE SPGW closes a P-CDR with a value of 24 before a switchover or with a value of 18 after a switchover during a PGW-to-SPGW mode change as part of an S1-base handover.

  This condition happens on the newly active gateway if an SPGW switchover occurs before a final modify bearer request comes to the SPGW to complete the S1-based handover.

  Workaround: There is currently no known workaround.

- CSCtx94033

When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

Workaround: Send the new create session request after the session is deleted.

- CSCty03462

  The Cisco LTE SPGW detects a Public Land Mobile Network (PLMN) change during a 3G-to-4G or 4G-to-3G handoff, and sets the PLMN ID change bit in the change condition for the service container.

  This condition occurs with an inter-routing access technology handoff.

  Workaround: There is currently no known workaround.

- CSCty76309

  The following error message displays in the gateway:

  ```
  %ADJ-3-ADJSTACK2: Adj stack2 error IPV6 midchain out of Virtual-Access5, addr
  2606:AE:C05D:7B2::C8 (incomplete): cannot stack on linktype requested: gtp tunnel st:
  ```

  This message displays with 100k IPv6 users and continuous IPv6 traffic with failover in between. The error message occurs during the switchover.

  Workaround: There is currently no known workaround.

- CSCtz55440

  The QCI status counters that display in the **show gprs qos status** command output do not increment on the standby gateway after a session is deleted.

  This condition occurs with an active-standby gateway configuration when a PDP is created and the same PDP is deleted on the standby gateway.

  Workaround: There is currently no known workaround.

- CSCua14402

  A handover request with a new path restart counter fails, but the path is restarted and the existing PDPs on the path are deleted.

  This condition occurs when a handover request to an existing path with new restart counter is dropped by the gateway.

  Workaround: Retransmit the handover request.

- CSCua92415

  The gateway crashes when the TCP link of the charging gateway goes down or flaps.

  This condition occurs when the path protocol configured is TCP and link up/down events occur, which trigger open and close socket events on a Cisco SAMI PowerPC (PPC), which also learns the link state information from other PPCs at the same time.

  Workaround: There is currently no known workaround.

- CSCua92426

  The standby Proxy Control Processor (PCOP) moves to STANDBY HOT before all of the Traffic and Control Plane processors (TCOPs).

  This condition occurs when the standby gateway comes up.

Workaround: There is currently no known workaround.

- CSCub25231

  The Aggregate Maximum Bit Rate (AMBR) is included in the Create PDP Response when it is not requested by the SGSN.

  This condition occurs when a create PDP context request does not contain an AMBR information element (IE).

  Workaround: There is currently no known workaround.

- CSCub25920

  Some of the handover counters do not increment properly in the **show gprs gtp statistics** command output.

  This condition occurs with the following counters:

  - P to SP change
    failed 0
  - P to GGSN change
    success 0
  - SP to GGSN change
    success 0
  - GGSN to SP change
    failed 0

  Workaround: There is currently no known workaround.

- CSCub84708

  The value for the "Total activated EPS Idle Sessions" counter in the **show gprs gtp status** command output is much higher than the value for the "Total activated sessions" counter.

  The "Total activated EPS Idle Sessions" counter is incorrectly incremented or decremented when the following conditions occur:

  - A handoff cancellation.
  - DSR after an initial attach.
  - Handover request came in without data path info.

  Workaround: There is currently no known workaround.

- CSCub95135

  A traceback occurs when the gateway is in a wait_ixp state and a get accounting response or Change of Authorization (COA) is received.

  When the gateway is in a wait_ixp state and an accounting response or COA is received, SM failure events will be posted and the session is deleted, which causes the traceback.

  Workaround: There is currently no known workaround.

- CSCuc11009

  The Cisco LTE SPGW crashes at "adj_switch_ipv4_generic_les" when processing downlink data packets.

  This condition occurs because of some inappropriate length in packet/calculations.

  Workaround: There is currently no known workaround.

- CSCuc11119

Spurious memory access is seen at “memory_ro_account_block_free.”

Workaround: There is currently no known workaround.

- CSCuc13861

  The gateway might crash with an “SCTP out of Window” message displayed on the console.

  This condition occurs during the re-assembly of data chunks and the transmission sequence number (TSN) of the chunk wrapped and became 0 (zero). The re-assembly logic failed and falsely indicated a gap in the message and the application was not signaled to read the message.

  Because of this, recv window was exhausted, resulting in the “SCTP out of window” message.

  Workaround: There is currently no known workaround other than rebooting the gateway.

- CSCuc30748

  The following syslog displays in the gateway:

  ```
  SAMI 11/3: Sep 21 16:20:22.954: %IPC-3-SAMI_SM_FAIL_DUP_MSISDN: Unexpected condition:
  TCOP in IMSI-Sticky doesn't match withMSISDN-Sticky MSISDN: 3DUf IMSI 804433445566110
  ```

  In a 3G-to-4G handoff scenario in which there is a CSReq without a mobile station ISDN (MSISDN) Informational Element (IE), when the same user moves to another Traffic and Control Plane processor (TCOP), the syslog displays.

  Workaround: There is currently no known workaround.

- CSCuc38645

  A Modify Bearer Request (MBR) without an S5/S8 Tunnel Endpoint ID (TEID) is incorrectly processed as a handoff.

  This condition occurs with the following scenarios:

  – Case1: MBR is rejected because of incorrect mandatory IE. This MBR is an invalid or old MBR delayed for some reason, which reaches the gateway after the PDP moved to GGSN-mode. When the PDP is in GGSN-mode, and an MBR without an SGW S5/S8 Fully Qualified Tunnel End Point Identifier (FTEID) is received, the system assumes this to be a GGSN-to-P handoff request and attempts to check for APN AMBR. It rejects the PDP because the perceived mandatory IE (APN AMBR) is missing.

  – Case2: During a P-to-SP handoff, when the PDP is in SPGW [HO] mode and the gateway wrongly receives an MBR from an old pat, the handoff is completed with the assumption the MBR is from a new path.

  Workaround: There is currently no known workaround.

- CSCuc41495

  The CSReq for SGW relocation is rejected with an incorrect mandatory IE.

  This condition occurs when the gateway already has a session in PGW-, GGSN-, or SPGW-mode with the same IMSI + EBI values, but the new CSR came for creating SGW portion. This issue will occur if there is a stale PDP on the GW.

  Workaround: There is currently no known workaround.

- CSCuc15645

  The gateway crashes when a problem with data removal occurs.

  Workaround: There is currently no known workaround.

- CSCuc58401

The gateway CDR MSTimezone trigger does not reset the current volume or time triggers for the UE.

This condition occurs only when MEF traffic switching is used for the session.

Workaround: Use CEF traffic switching.

- CSCuc83309

  High CPU usage is seen in the gateway when packets that are denied in an access list are process switched.

  Workaround: Remove the access list so that packets are MEF switched

- CSCuc84183

  The following traceback is seen:

```
SAMI 4/8: 006605: Oct 23 12:03:33: %ALIGN-3-SPURIOUS: Spurious memory access made at
0x9E9A644z  reading 0x4
SAMI 4/8: 006606: Oct 23 12:03:33: %ALIGN-3-TRACE: -Traceback= 0x9E9A644z 0x9E9A5ECz
0x9EA42F0z 0x9EB0760z 0x83145B4z 0x99D792Cz 0x99DB0B4z 0x0z
SAMI 4/8: 006607: Oct 23 12:03:33: %ALIGN-3-TRACE: -Traceback= 0x9E9A648z 0x9E9A5ECz
0x9EA42F0z 0x9EB0760z 0x83145B4z 0x99D792Cz 0x99DB0B4z 0x0z
SAMI 4/8: 006608: Oct 23 12:03:33: %ALIGN-3-TRACE: -Traceback= 0x9EA7A50z 0x97B8E10z
0x97B8F40z 0x9E5D770z 0x83145E4z 0x99D792Cz 0x99DB0B4z 0x0z
```

  This traceback is seen while processing Downlink Data Notification (DDN) Ack message during a Gtpv2 iRAT handover.

  Workaround: There is currently no known workaround.

- CSCuc84209

  The following syslog and traceback is seen on the active Cisco LTE SPGW:

```
SAMI 1/8: 000352: Oct 17 16:30:46: %GTP-7-GWDEBUG: PDP:0x065D100C, refcnt:0, Wrong
refcnt when charging_reserved,  -Traceback= 0x834586Cz 0x82C7004z 0x8054194z
0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000353: Oct 17 16:31:29: %ALIGN-3-SPURIOUS: Spurious memory access made at
0x82C5EC0z  reading 0xD4
SAMI 1/8: 000354: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C5EC0z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000355: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x8304178z 0x82C5F18z
0x82C6FE8z 0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz
SAMI 1/8: 000356: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C60A8z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000357: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x82C6150z 0x82C6FE8z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
SAMI 1/8: 000358: Oct 17 16:31:29: %ALIGN-3-TRACE: -Traceback= 0x83456F0z 0x82C7004z
0x8054194z 0x82DA250z 0x88E408Cz 0x8026FB8z 0x99D792Cz 0x99DB0B4z
```

  The syslog and traceback is seen on active SPGW during the execution of the **show gprs gtp pdp-context tid all** command.

  Workaround: There is currently no known workaround.

- CSCuc84491

  For reasons not yet determined, the following syslog might be seen:

```
SAMI 1/7: 006401: Oct 23 15:23:35: %SYS-2-BADSHARE: Bad refcount in pak_enqueue,
ptr=209F3BB8, count=0,  -Traceback= 0x997BC94z 0x997D914z 0x8321C5Cz 0x9DE3660z
0x9E9FEC4z 0x9EA4074z 0x9EB0760z 0x83145B4z 0x99D792Cz 0x99DB0B4z SAMI 1/7: 006402:
Oct 23 15:23:35: %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=209F3BB8,
count=0,  -Traceback= 0x9976888z 0x997DB04z 0x8321C5Cz 0x9DE3660z 0x9E9FEC4z
0x9EA4074z 0x9EB0760z 0x83145B4z 0x99D792Cz 0x99DB0B4z
```

Workaround: There is currently no known workaround.

- CSCuc90802

  The following syslog is seen during the deletion of a PDP when the update PDP synchronization on the standby gateway failed because of a sync decode failure:

  GTP-7-GTPPDPSTATE: GTP: PDP check:

  Workaround: There is currently no known workaround.

- CSCuc98212

  The Cisco LTE SPGW crashes due to an unexpected exception to CPU.

  This condition occurs when an MBR for a GTPv1-to-GTPv2 handoff with “Bearer Context to be removed” in the message is received.

  Workaround: There is currently no known workaround.

- CSCud04466

  The Cisco LTE SPGW crashes due to an Uunexpected exception to CPU.

  This condition occurs with the Cisco IOS Cisco Express Forwarding (CEF) feature after prolonged stress conditions.

  Workaround: There is currently no known workaround.

- CSCud05773

  The Cisco LTE SPGW crashes with an Unexpected exception to CPU.

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

- CSCud09932

  The Cisco LTE SPGW crashes with “CPU exception.”

  This crash occurs during P- to SP-mode handover while the gateway is processing a CSR message.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4i.

- 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 occasion 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.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

Workaround: There is currently no known workaround.

- CSCua36249

  When an Xscale CPU reload occurs because of a QNX crash, the Cisco SAMI network processor (IXP) console displays the reload reason as UNKNOWN (IXP CAUSE = NP Core Reset - Cause Unknown).

  This condition occurs when there is a QNX microkernel crash on the Xscale CPU.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4i. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 77
- Cisco SAMI Resolved Caveats, page 82

Cisco LTE SPGW Resolved Caveats

This section lists SPGW-specific caveats that are resolved in Cisco IOS Release 12.4(24)T4i.

- CSCtx82331

  Spurious memory access reading “0x5C.”

  This condition is seen during an X2 handoff with SGW relocation when the Cisco LTE SPGW is waiting to receive an SCU and DSR with the scope indication bit set.

- CSCty27743

  The gateway sends the incorrect sequence number 0 (zero) in the response message to the Indirect Data Fwd Request from the MME.

  This condition occurs in all response messages for the Create Indirect Data Forward Tunnel request from the MME. The gateway might accept the request, but because of the incorrect sequence number in the response, the MME is unable to correlate the response with the request.

- CSCtz44171

  The “Total Activated EPS idle Sessions” counter in the **show gprs gtp status** command output increments while opening a a GTVv2 PDP (CSR with no S1-U Fully Qualified Tunnel End Point Identifier [FTEID]). This counter should increment only after an RAB deletes an existing S1-U path.

  This condition occurs only with a GTPv2 PDP initial attach.

- CSCua09583

  The charging information element (IE) is invalid on the standby gateway. This condition occurs when the charging IE is received in a Modify Bearer Request (MBR).

- CSCua20789

  Multiple tracebacks on the standby gateway are observed. This condition occurs after the gateways have been up for at last one week and are possibly related to multiple handoffs for the same session.

  Additionally, the path was not available under the PDP, hence the observed tracebacks. This condition does not impact any of the users or sessions.

- CSCub53325

A dual APN session handoff fails with gateway relocation. When dual APN is not enabled, a session handoff with gateway relocation works without issue.

This condition occurs only with a session handoff failure with gateway relocation with dual APN enabled.

- CSCub59169

  Spurious memory access is made with reading 0xC while a PDP in SGW-mode is processing a DSR.

  This condition occurs when an SGW-mode PDP with missing SGW context and DSR message is received with the OI bit set or received without the OI bit set but for an idle state PDP.

- CSCub90100

  The standby gateway crashes while processing a Modify Bearer Request (MBR) with no data path.

  This crash occurs under the following conditions:

  - Create a GTPv1 PDP with an SGSN1 address
  - Create a GTPv2 PDP with an MME1 address (SP mode) - S1
  - Create a GTPv2 PDP with an MME2 address (SP mode) - S2
  - Send an RAB to S1 and wait for the data path to be removed from the standby gateway (60 seconds)
  - Delete an S2 PDP and wait for the MME2 path (both signal and data) to be removed from the standby gateway (60 seconds)
  - Create the S2 PDP again with the MME2 address
  - Now do a GTPv1 handoff for the S1 PDP to the SGSN1 address (not the new SGSN)

  The standby gateway crashes while handling the MBR with no data path.

- CSCub90201

  A path timer is not working as expected, which causes a gateway crash.

  This condition occurs when a path timer is not working as expected.

- CSCub90222

  The path of an active SPGW crashes with a Modify Bearer Signaling request.

  This condition occurs when a standby gateway becomes active and attempts to handle an incomplete SPGW-mode PDP.

- CSCub90299

  An IO memory corruption crash occurs because of a GTP-U data packet corruption in memory.

  This condition might be caused by incorrect writing of a CDR container to the memory.

- CSCub91514

  The Cisco LTE SPGW reloads while receiving a RAB request. This condition occurs during the SP-to-GTPv1 handoff when an RAB request is received when the handoff is in progress.

- CSCub93416

  When two Cisco LTE SPGWs are acting as SGW and PGW gateways mutually, new session creation fails on the SPGWs.

  This condition occurs with the following:

  - SPGW-1 and SPGW-2 has SGW-mode and PGW-mode sessions respectively for a user.

    - An attempt to create a session for another user fails when SPGW-2 acts as SGW-mode and SPGW-1 acts as PGW-mode (reverse of that in point 1).
- CSCub93774

  The active Cisco LTE SPGW reloads while processing 3G-to-4G handover in the following specific case:

    - There is a 4G session on the SPGW and the MME has specified a few protocol configuration options in PCO IE in the initial attach.
    - The active gateway reloads for some reason and the new active gateway later receives the Modify Bearer Request (MBReq) from the S4-SGSN for handover.
    - The gateway reloads while sending an MBResp to the S4-SGSN.
- CSCub94102

  A crash occurs with an SP-to-GGSN handoff followed by a DSR with priv-ext information element (IE).

  This condition occurs with the following:

    - Create a GTPv2 session in SP-mode
    - Handoff to GTPv1 3G call and mode is GGSN
    - Send a DSR with a private extension
- CSCub95059

  Spurious memory access while sending DSR with ECGI ULI.

  This condition occurs when a DSR is received with ECGI ULI while doing a 4G-to-3G handoff.
- CSCub99539

  There is no syslog for an inconsistent PDP state on the standby gateway after synchronization.

  This condition occurs with an incomplete SPGW-mode PDP on the standby gateway after the standby becomes ACTIVE and it attempts to handle the Modify Bearer Request, which results in a crash.
- CSCuc01850

  The gateway crashes when if receives a lot of MBRs and RABs with the same sequence number.
- CSCuc03670

  The gateway crashes when a corrupted HI3 LI packet arrives at the gateway and causes illegal IO memory.

  This condition occurs when an LII data packet (HI3) with an inner IP length less than the GTP length is tapped at the gateway, which causes the LI memory corruption.
- CSCuc03972

  A GTPv1-to-GTPv2 PDP handover (PGW-mode) and back to GTPv1 fails on the gateway if there is a redundancy switchover in between.

  This condition occurs with the following:

    - Create a GTPv1 PDP.
    - Handover it to GTPv2 (PGW-mode).
    - Perform a switchover so that the standby SPGW becomes the active gateway.

  The PDP handover to GTPv1 fails.

- CSCuc08100

  The Cisco LTE SPGW crashes when it receives an RAB request without an EBI list when it has both GTPv1 and GTPv2 sessions for same IMSI under different APNs.

- CSCuc08363

  When the Cisco LTE SPGW is already in a downlink data path blocked state, and data path removal event is synced from the active gateway to the standby gateway, the following syslog is seen on the standby SPGW:

  ```
  FSM failed: Bearer state not changed to Blocked state" syslog is seen on the standby SPGW.
  ```

- CSCuc08622

  A GTPv2 session is not accessible through control messages from the MME/s4-SGSN.

  This condition occurs when two multi-PDN GTPv2 sessions exist for same the IMSI and only one of them is handed off to GTPv1. The remaining Gtpv2 session is not accessible via control messages.

- CSCuc08812

  While processing DSR to clear S portion during an SP-to-P handover for multi PDN session scenario, multiple spurious access reading 0x5C is seen.

- CSCuc08822

  When a GTPv1 and GTPv2 call is created for a user and both calls “land” on same Traffic and Control Plane processor (TCOP), while deleting the sessions, the IMSI-sticky is sometimes not cleared properly. Therefore, if the same user lands on another TCOP when the user creates a third call, the following syslog is seen:

  ```
  %IPC-3-SAMI_SM_FAIL_DUP_MSISDN: Unexpected condition
  ```

- CSCuc10523

  A crash occurs when running “check heaps” after a memory corruption.

- CSCuc10690

  A crash occurs at “spgw_mbr_backup_sig_path.”

- CSCuc10825

  A multiple spurious access reading 0xC is seen.

  This traceback occurs during the cancellation of a P-to-SP handover when the handoff to SP is in progress and DSR is received with the SI flag set.

- CSCuc11478

  The Cisco LTE SPGW does not send a Downlink Data Notification (DDN) in a multi PDN handoff scenario.

  This condition occurs with the following sequence of events:

  - Two SP mode sessions.
  - Second session does not have S1-U.
  - First session is handed over to GTPv1.
  - Downlink data arrives for the second session.
  - The gateway triggers DDN.

Until the first session is in interim HO mode, DDN for the second session is forwarded; however, after a complete handoff, DDN for the second session in not forwarded.

- CSCuc15847

  The active Cisco LTE SPGW reloads when a Modify Bearer Request from a Mobility Management Entity (MME) reaches the serving gateway (SGW) after a GTPv2-to-GTPv1 handoff.

  This condition occurs with the following scenario:

  - Two SPGW-mode sessions from same user exist in SPGW.
  - One of these sessions is handed off into GTPv1.
  - A GTPv2 message arrives on the GTPv1 session with the SGW Tunnel Endpoint Identifier (TEID).

- CSCuc16875

  Incompatible CDR with customer charging gateway.

  This condition occurs wen Cisco LTE SPGW Release 2 sends a Fully Qualified Domain Name (FQDN) in the call detail record (CDR) as opposed to a short APN name, causing issues with the charging gateway.

- CSCuc21347

  A traceback is seen in the active gateway while sending an Update-Context-Request for a GTPv1 PDP.

  This condition occurs because the LTE handoff flag is set during the GTPv2-toGTPv1 handoff and does not get cleared even after the handoff is successful. Therefore, a subsequent Update Context Request message results in spurious memory access.

- CSCuc25282

  A traceback is seen with “sgw_gtpv2_msg_processing+0xc94.”

  This “sgw_gtpv2_msg_processing+0xc94” traceback is seen while processing a GTPv2 message with a Tunnel Endpoint Identifier of 0 (zero).

- CSCuc28643

  The gateway crashes due to “chunk” corruption where the chunk name points to “GTP to be del.”

  This condition occurs during multiple handoffs at high rate.

- CSCuc39773

  The gateway crashes when an SGW-mode PDP receive an MBR with a different EBI value than the existing one.

  This condition occurs when the Mobile Management Entity (MME) is wrongly sending a different EBI value in the MBR than the EBI value of the existing session. This can happen in a multi-PDN scenario, where the MME thinks it has two sessions with SGW and sends MBR for both sessions, and the SGW has only one session. The MBR with the current session's EBI is processed correctly, and when the gateway attempts to process the MBR with a different EBI value on the same IMSI, the gateway crashes.

- CSCuc92127

  A session uses Cisco Express Forwarding (CEF) even though it has been configured for Mobile Express Forwarding (MEF).

When this condition occurs, the packet is CEF switched. All PDPs in the path/remote address in the Traffic and Control Plane processors (TCOP) where the path is stale are affected. This continues to occur until the stale entry is removed. For the same path/remote address, sessions in other TCOPs are NOT affected.

Cisco SAMI Resolved Caveats

The following Cisco SAMI caveats are resolved with Cisco IOS Release 12.4(24)T4i.

- CSCtw60993

  The Cisco SAMI reloads with the following syslog 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 information, the core file "qnx_1_io-net_*xxxx*_core" is generated, where *xxxx* is the process-id for io-net and might vary from case-to-case.

  The conditions under which this reload and syslog error message occur are unknown.

- CSCty65255

  When the **show sami temperature** and the **show environment temperature** are executed, different temperatures display in the command output for all of the columns except for the base board sensors 0 and 1.

  This condition is caused by the **show sami temperature** reading the wrong values from the destined address for temperature.

Unreproducible Caveat

The following Cisco LTE SPGW caveat has not been reproduced in Cisco IOS Release 12.4(24)T4i.

- CSCua81225

  Stuck PDPs are observed on the gateway.

  This condition occurs while running a large number of 3G and 4G create subscriber sessions, sending traffic, and then deleting all the sessions.

Caveats - Cisco IOS Release 12.4(24)T4h

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1e, Cisco IOS Release 12.4(24)T4h image:

- Open Caveats, page 82
- Resolved Caveats, page 86
- Unreproducible Caveat, page 87

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 83
- Cisco SAMI Open Caveats, page 85

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4h.

- CSCtf14093

  Network Management System (NMS) poll on CISCO-IP-LOCAL-POOL-MIB does not provide IPv6 local pool entries.

  This condition is seen when an SNMP poll is done on CISCO-IP-LOCAL-POOL-MIB from Mobile Wireless Transport Manager (MWTM) or any other NMS. As a result of this condition, monitoring IPv6 local pools via an NMS not possible.

  Workaround: There is currently no known workaround.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx91844

  The “S1/X2 change counter” does not increment in the **show gprs gtp statistics** command output after a handover.

  This condition is seen with the following scenario:

  a. S1 with no SGW change.
  b. S1 with an SGW change.
  c. X2 with no SGW change.
  d. X2 with an SGW change.

  Additionally, the S1 and X2 counters are calculated incorrectly; therefore, they are not serving the purpose for which they are intended. The S1 and X2 counters generate incorrect information while debugging as well.

  Workaround: There is currently no known workaround.

- CSCtx93599

  The Cisco LTE SPGW closes a P-CDR with a value of 24 before a switchover or with a value of 18 after a switchover during a PGW-to-SPGW mode change as part of an S1-base handover.

  This condition happens on the newly active gateway if an SPGW switchover occurs before a final modify bearer request comes to the SPGW to complete the S1-based handover.

Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCty03462

  The Cisco LTE SPGW detects a Public Land Mobile Network (PLMN) change during a 3G-to-4G or 4G-to-3G handoff, and sets the PLMN ID change bit in the change condition for the service container.

  This condition occurs with an inter-routing access technology handoff.

  Workaround: There is currently no known workaround.

- CSCua14402

  A handover request with a new path restart counter fails, but the path is restarted and the existing PDPs on the path are deleted.

  This condition occurs when a handover request to an existing path with new restart counter is dropped by the gateway.

  Workaround: Retransmit the handover request.

- CSCua20789

  Multiple tracebacks are observed on a standby gateway that has been up for at least a week. This condition might have occurred during multiple handoffs for the same session. A path was not available under the PDP, hence the observed tracebacks.

  This condition does not impact sessions

  Workaround: There is currently no known workaround.

- CSCua81225

  Stuck PDPs are observed on the gateway.

  This condition occurs while running a large number of 3G and 4G create subscriber sessions, sending traffic, and then deleting all the sessions.

  Workaround: There is currently no known workaround.

- CSCua92415

  The gateway crashes when the TCP link of the charging gateway goes down or flaps.

  This condition occurs when the path protocol configured is TCP and link up/down events occur, which trigger open and close socket events on a Cisco SAMI PowerPC (PPC), which also learns the link state information from other PPCs at the same time.

  Workaround: There is currently no known workaround.

- CSCua92426

  The standby Proxy Control Processor (PCOP) moves to STANDBY HOT before all of the Traffic and Control Plane processors (TCOPs).

  This condition occurs when the standby gateway comes up.

Workaround: There is currently no known workaround.

- CSCub25231

  The Aggregate Maximum Bit Rate (AMBR) is included in the Create PDP Response when it is not requested by the SGSN.

  This condition occurs when a create PDP context request does not contain an AMBR information element (IE).

  Workaround: There is currently no known workaround.

- CSCub25920

  Some of the handover counters do not increment properly in the **show gprs gtp statistics** command output.

  This condition occurs with the following counters:

  - P to SP change
    failed 0
  - P to GGSN change
    success 0
  - SP to GGSN change
    success 0
  - GGSN to SP change
    failed 0

  Workaround: There is currently no known workaround.

- CSCub53325

  A dual APN session handoff fails with an SGW relocation while a session handoff with an SGW relocation works as designed without dual APN enable.

  This failure is seen only when a dual APN is enabled.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4h.

- 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 occasion 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.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

Workaround: There is currently no known workaround.

- CSCua36249

  When an Xscale CPU reload occurs because of a QNX crash, the Cisco SAMI network processor (IXP) console displays the reload reason as UNKNOWN (IXP CAUSE = NP Core Reset - Cause Unknown).

  This condition occurs when there is a QNX microkernel crash on the Xscale CPU.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4h. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 86
- Cisco SAMI Resolved Caveats, page 87

Cisco LTE SPGW Resolved Caveats

This section lists SPGW-specific caveats that are resolved in Cisco IOS Release 12.4(24)T4h.

- CSCtx94845

  After a pre-Release 8 SGSN-to-S4 SGSN handover, the Cisco LTE SPGW retains the pre-Release 8 SGSN path, even after all the sessions are removed.

  This condition occurs when the switchover occurs before the old SGSN path is removed due to a path cleanup timer expiration after a GTPv1-to-GTPv2 handover on the active gateway.

- CSCua20990

  A traceback is seen while service records are added during call detail record closure.

  This condition occurs when the SCR is not sent by the gateway for any of the Gn triggers when interim accounting is disabled under an APN.

- CSCua38505

  The following syslog message is observed on the standby gateway:

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

  This condition occurs if a Traffic and Control Processor (TCOP) path deletion synchronization is delayed and the same time another TCOP begins to sychronize the same path. When this condition occurs, the existing path handle is overwritten by a new handle and the previous handle is not released, which causes the ID leak.

- CSCua85225

  The active gateway crashes while processing a GTPv2 Modify Bearer Request.

  Under a specific circumstance, a failure while processing the Modify Bearer Request could lead to a memory corruption in peer-node Called-Station-ID (CSID) attribute of the session. This memory corruption could lead to a crash.

- CSCua87327

  Session creation attempts from new SGSN/MME fail if total GTPv1-U data paths on LTE GW exceeds 4K.

- CSCub04146

The gateway crashes due to a “SGW MCB Context” chunk corruption.

This condition occurs when a Traffic Flow Template (TFT) size greater than 255 is sent in a create session request to the SGW or is received in a create session response.

- CSCub09677

  When trying to create a session when an IP pool is not available, the gateway displays “Failed to allocate prefix on virtual-access” without sending a create session reject (CSReject) with no resource available.

  This condition occurs while creating IPv6 multi-PDN connections.

- CSCub11204

  The gateway does not check for the “No QOS Negotiation” common flag.

  Regardless, the gateway sends the SGSN/SGW the negotiated QOS value even though the common flag is set to “No QOS Negotiation.”

Cisco SAMI Resolved Caveats

There are no new Cisco SAMI caveats resolved with Cisco IOS Release 12.4(24)T4h.

Unreproducible Caveat

The following Cisco LTE SPGW caveat has not been reproduced in Cisco IOS Release 12.4(24)T4h.

- CSCtw60993

  The Cisco SAMI reloads with the following syslog 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 crash information, core file “qnx_1_io-net_114693_core” is generated. “114693” is the Process ID for io-net, which might vary from case-to-case. There are no known issues that might result in this issue.

Caveats - Cisco IOS Release 12.4(24)T4g

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1d, Cisco IOS Release 12.4(24)T4g image:

- Open Caveats, page 87
- Resolved Caveats, page 90

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 88

- Cisco SAMI Open Caveats, page 89

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4g.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx91844

  The "S1/X2 change counter" does not increment in the **show gprs gtp statistics** command output after a handover.

  This condition is seen with the following scenario:

  a. S1 with no SGW change.
  b. S1 with an SGW change.
  c. X2 with no SGW change.
  d. X2 with an SGW change.

  Additionally, the S1 and X2 counters are calculated incorrectly; therefore, they are not serving the purpose for which they are intended. The S1 and X2 counters generate incorrect information while debugging as well.

  Workaround: There is currently no known workaround.

- CSCtx93599

  The Cisco LTE SPGW closes a P-CDR with a value of 24 before a switchover or with a value of 18 after a switchover during a PGW-to-SPGW mode change as part of an S1-base handover.

  This condition happens on the newly active gateway if an SPGW switchover occurs before a final modify bearer request comes to the SPGW to complete the S1-based handover.

  Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCtx94845

After a pre-Release 8 SGSN-to-S4 SGSN handover, the Cisco LTE SPGW retains the pre-Release 8 SGSN path, even after all the sessions are removed.

This condition occurs when the switchover occurs before the old SGSN path is removed due to a path cleanup timer expiration after a GTPv1-to-GTPv2 handover on the active gateway.

Workaround: There is currently no known workaround.

- CSCty03462

  The Cisco LTE SPGW detects a Public Land Mobile Network (PLMN) change during a 3G-to-4G or 4G-to-3G handoff, and sets the PLMN ID change bit in the change condition for the service container.

  This condition occurs with an inter-routing access technology handoff.

  Workaround: There is currently no known workaround.

- CSCua20789

  Multiple tracebacks are observed on a standby gateway that has been up for at least a week. This condition might have occurred during multiple handoffs for the same session. A path was not available under the PDP, hence the observed tracebacks.

  This condition does not impact sessions

  Workaround: There is currently no known workaround.

- CSCua20990

  A traceback occurs when service records are added during the closure of call detail records (CDRs)

  This condition occurs with SPGW or GGSN mode sessions with Cisco LTE SPGW Release 2.2.1b and Release 2.2.1c.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4g.

- 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 occasion 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.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4g. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 90
- Cisco SAMI Resolved Caveats, page 92

Cisco LTE SPGW Resolved Caveats

This section lists SPGW-specific caveats that are resolved in Cisco IOS Release 12.4(24)T4g.

- CSCtz32489

  The following cases fail with the Cisco LTE SPGW and Cisco ASR 5000 Series Packet Data Network Gateway (PGW).

  - Evolved UTRAN (EUTRAN)-to-Universal Terrestrial Radio Access Network (UTRAN) handover with SGW relocation.
  - UTRAN-to-EUTRAN handover with SGW relocation.
  - EUTRAN-to-GSM/EDGE Radio Access Network (GERAN) handover with SGW relocation.
  - GERAN-to-EUTRAN handover with SGW relocation.
  - S1 handover with SGW relocation.

  These cases fail only with the Cisco ASR5000 series gateway because the Cisco LTE SPGW SGW function expects the Linked EPS Bearer ID (LBI) to be added in the above cases when it is actually not needed. Because the Cisco LT E PGW adds the LBI response in the above cases, the cases do not fail with the Cisco LTE PGW.

- CSCtz68967

  The PDP counters under an APN display an incorrect non-zero value when there are no existing sessions present in the system.

  This condition occurs when there is a path failure while a 3G-to4G handoff is in progress

- CSCtz70209—MME to S4-SGSN RAU SPGW should not reply with 1kbps AMBR value
- CSCtz83909

  Path echo messages, downlink notification messages, and update bearer requests triggered by the network fail because the Mobility Management Entity (MME) is expecting IPv4 instead of IPv6.

  This condition occurs with the following scenario:

  a. With the Create Session Request (CSR), the MME sends both IPv4 and IPv6 addresses for the S11 MME GTP-C.
  b. When both IPv4 and IPv6 addresses are present for the MME, the SGW sets the S11 path using the IPv6 address.
  c. The CSResp sends an IPv6 Fully Qualified Tunnel End Point Identifier (FTEID) when the MME is expecting IPv4.

- CSCua21522

  The standby gateway might reload (RF-induced) because of an Stream Control Transmission Protocol (SCTP) “out of window” issue.

This condition occurs when the SCTP stack runs out of receive window space and is unable to accommodate additional data from the active gateway. This occurs during periods of high stress load conditions.

- CSCua22824

  The Cisco LTE SPGW crashes when sending a Modify Bearer Request (MBR) for a GTPv1-to-GTPv2 handoff.

  This condition occurs when a user has dual APN GTPv1 PDPs and one of the sessions is handed over to GTPv2 without a data path. If downlink data arrives for this GTPv2 session, the gateway triggers a Downlink Data Notification (DDN) towards the Mobility Management Entity (MME). If N3T3 timer times out for the DDN, the active gateway crashes.

  Specifically, this condition occurs with the following scenario:

  a. Two GTPv1 PDPs are created for the same International Mobile Subscriber Identity (IMSI) and different APNs (multiple PDNs).
  b. One of the GTPv1 PDPs is handed over to GTPv2 by sending a CSReq without a data path.
  c. Downlink traffic is sent GTPv2 PDP, which triggers the DDN.
  d. When the DDN N3T3 timer times out, the gateway crashes.

- CSCua07639

  Quality of Service (QoS) shared by the Policy Control and Charging Rules Function (PCRF) is not sent to the Mobility Management Entity (MME) when a Tracking Area Update (TAU) occurs.

  This condition occurs with the following scenario:

  a. The MME sends a TAU to the gateway.
  b. The gateway sends an Acct-Interim to the Cisco CSG2 with “coa_flags=0x09” instead of “0x03”
  c. The CSG2 sends CCR-U to PCRF and obtains new QoS from PCRF in a CCA-U.
  d. The CSG2 does *not* initiate Change of Authorization (COA) to the gateway because the gateway sent an interim update with the COA flag as 0x09. Therefore, the gateway does not initiate an Update Bearer Request to the MME.

- CSCua27601

  The following syslog message is observed on the standby SPGW:

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

  This message could be triggered in certain error scenarios in which a PDP ID is not freed when the PDP is deleted.

- CSCua11147

  The Certificate Configuration Message (CCM) maximum buffer size is 8k. In the event the return buffer size is greater than the CCM maximum buffer size (for example, the CSReq, MBreq, etc.), the gateway displays a syslog message and drops the request.

- CSCua22497

  A race condition occurs with an Update Bearer Request (UBR).

  The condition occurs during an S4- to S11- handover (from the SGSN to the Mobility Management Entity [MME]), when the MME sends the first Modify Bearer Request (MBR) with no S1-U Fully Qualified Tunnel End Point Identifier (FTEID). Because of a QoS change request from the Policy Control and Charging Rules Function (PCRF) side, the SGW sends an Update Bearer Request to the

MME. The MME does not respond to the request and at the same time, the MME sends a Modify Bearer Request, to which SGW does not respond because it is waiting for the UBR response, which results in a deadlock.

- CSCua57370

  The Cisco LTE SPGW sends a Downlink Data Notification (DDN) to the S4-SGSN when a user plane Tunnel Endpoint Identifier (TEID) exists. This behavior occurs because the Mobility Management Entity (MME) sends a Radio Access Bearer (RAB) assignment request after completion of a handoff and the gateway is deleting the user plane after receving the RAB assignment request. The gateway should not delete the user plane if it recevies an RAB from a wrong node.

- CSCua70464

  The CPU usage spikes on both the Proxy Control Processor (PCOP) and the Traffic and Control Plane processors (TCOPs) when there are large number of GTP paths on the gateway.

  This increased CPU usage occurs with the following conditions:

  a. Total number of GTP paths on the gateway is very large (approximately 6000 or 7000 paths).
  b. GTP echo messages are arriving at a high rate.
  c. Continuous PDP/session creation or deletion is occurring at high rate.

Cisco SAMI Resolved Caveats

The following Cisco SAMI caveats are resolved with Cisco IOS Release 12.4(24)T4g.

- CSCtz07383

  An unexpected termination of the XScale qconn process on a Cisco SAMI IXP XScale processor might cause the Cisco SAMI to reload. Issuing the **show version** command on the Cisco SAMI PowerPCs (PPCs) after the reload displays the following:

  ```
  System returned to ROM by NP 1 Failed : NP Core Reset - Cause Unknown at <timestamp>
  ```

  Currently, no specific conditions are known to cause the unexpected termination of the qconn process.

- CSCtz37598

  When a Cisco SAMI reloads because of an IXP Health Monitoring failure triggered by IXP SRAM parity or an DRAM error correcting code (ECC) error, the crashinfo for the IXP that encountered the SRAM/DRAM error is not present in the crashinfo_collection.tar file.

  This condition occurs only if the SAMI reloads because of an IXP SRAM parity or DRAM ECC error.

Caveats - Cisco IOS Release 12.4(24)T4f

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1c, Cisco IOS Release 12.4(24)T4f image:

- Open Caveats, page 93
- Resolved Caveats, page 95
- Unreproducible Caveat, page 96

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 93
- Cisco SAMI Open Caveats, page 94

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4f.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx91844

  The "S1/X2 change counter" does not increment in the **show gprs gtp statistics** command output after a handover.

  This condition is seen with the following scenario:

  a. S1 with no SGW change.
  b. S1 with an SGW change.
  c. X2 with no SGW change.
  d. X2 with an SGW change.

  Additionally, the S1 and X2 counters are calculated incorrectly; therefore, they are not serving the purpose for which they are intended. The S1 and X2 counters generate incorrect information while debugging as well.

  Workaround: There is currently no known workaround.

- CSCtx93599

  The Cisco LTE SPGW closes a P-CDR with a value of 24 before a switchover or with a value of 18 after a switchover during a PGW-to-SPGW mode change as part of an S1-base handover.

  This condition happens on the newly active gateway if an SPGW switchover occurs before a final modify bearer request comes to the SPGW to complete the S1-based handover.

  Workaround: There is currently no known workaround.

- CSCtx94033

When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

Workaround: Send the new create session request after the session is deleted.

- CSCtx94845

  After a pre-Release 8 SGSN-to-S4 SGSN handover, the Cisco LTE SPGW retains the pre-Release 8 SGSN path, even after all the sessions are removed.

  This condition occurs when the switchover occurs before the old SGSN path is removed due to a path cleanup timer expiration after a GTPv1-to-GTPv2 handover on the active gateway.

  Workaround: There is currently no known workaround.

- CSCty03462

  The Cisco LTE SPGW detects a PLMN change during a 3G-to-4G or 4G-to-3G handoff, and sets the PLMN ID change bit in the change condition for the service container.

  This condition occurs with an inter-routing access technology handoff.

  Workaround: There is currently no known workaround.

- CSCtz68967

  The PDP counters under an APN display an incorrect non-zero value when there are no existing sessions present in the system.

  This condition occurs when there is a path failure while a 3G-to4G handoff is in progress

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4f.

- 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 occasion 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.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4f. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 95
- Cisco SAMI Resolved Caveats, page 96

Cisco LTE SPGW Resolved Caveats

This section lists SPGW-specific caveats that are resolved in Cisco IOS Release 12.4(24)T4f.

- CSCto99780

  The gateway crashes because of a rare condition that occurs while processing a Modify Bearer Request for an SGW change.

  This condition occurs when the active SPGW has crashed because of a race condition that occurred when the gateway failed to set up new data path parameters.

- CSCtw60222

  The following hardware failure notice is seen on the LCP:

  ```
  %SAMI-3-730205: SAMI User Space: ERROR: Proc-3 hw watchdog timeout event received
  %SAMI-3-730205: SAMI User Space: ERROR: lcp handle ppc crash notice for proc 3
  %SAMI-5-730203: SAMI User Space: Notice: Reload reason: Proc 3 - hw watchdog failure
  ```

  No specific conditions appear to trigger the failure notice; however, any process that has disabled interrupts for more than three seconds appears to trigger the failure notice.

- CSCtx81773

  A memory leak of 276 bytes is seen in the certificate configuration message (CCM) process on the standby SPGW.

  This condition occurs when memory is allocated during the closure of a call detail record (CDR) for an internal charging request/response message.

- CSCtx82290

  A continuous or looping output occurs when the **show sami sm imsi** privileged EXEC command is issued on PPC3. The PPC3 CPU usage remains high despite even after executing “Ctrl+Shift+6.”

  This condition occurs when both GTPv1 and GTPv2 sessions exist on the gateway and the **show sami sm imsi** command is executed on PPC3.

- CSCtx94985

  A negative value is seen for the “Total activated GTPv1 PDPs” counter that displays in the **show gprs gtp status** command output.

  This condition occurs when a CSR for handoff is received by the gateway for a PDP that is in a deleting state and waiting for a final Service Control Usage (SCU) to complete deletion, and the gateway begins processing the CSR and progresses the session to SPGW[HO].

  Moving the session to SPGW[HO] increments the “Total activated GTPv2 EPS bearers” counter and decrements the “Total activated GTPv1 PDPs” counter. Then, when the final SCU is received, the gateway decrements the “Total activated GTPv1 PDPs” counter once again, which leads to a negative value.

- CSCty31897

The gateway might not respond to a Modify Bearer Command message from the Mobility Management Entity (MME).

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

- CSCty55350

  When an IPv6 subscriber user disconnects and attempts to reconnect, an error message is seen on the reconnect attempt. This error message is seen only when the IPv6 MTU is great than 1432.

- CSCty77869

  When an IPv6 Neighbor Discovery (ND) message is sent, a traceback is seen on the data path. This condition occurs only outside of normal operating parameters and is reproduced with the scenario in which an immediate PDP create, delete, and create occurs, but is not always seen. This condition is a transient one in which the IPv6 ND background process is trying to send a router advertisement to a UE, for which the data path is not valid because the data path was removed or not successfully established

- CSCty96931

  The gateway might report DFP weight as zero (0) to the IOS SLB and become throttled. This condition occurs when the bearer metric value reported by the Traffic and Control Plane processors (TCOPs) on the gateway is 0.

  This issue is seen only when a very high number of GTPv2-to-GTPv1 handoffs occur and the sum of the current active sessions plus the GTPv2-to-GTPv1 handoff counts exceed the maximum bearer capacity configured for the gateway.

- CSCtz30894

  The active gateway crashes during a rare scenario in which the N3 + T3 timeout occurs for a Downlink Data Notification (DDN) message by the gateway towards the Mobility Management Entity (MME) while a GTPv1-to-GTPv2 handoff in progress for a session fails on the gateway.

- CSCtz43041

  Link Bearer Identity (LBI) Information Element (IE) is missing in the Create Session Response during 3G-to-4G Inter-Radio Access Technology (iRAT) handover. Because the LBI is missing, the MME treats the Create Session Response as a handover failure.

  This condition occurs when there is a handover request for Gn/Gp SGSN to MME and the Create Session Response does not contain the LBI IE.

- CSCtz54485

  The “gtpv2_initiated_bearer” counter does not decrement after PDPs are locally cleared.

  This condition exists when the **clear gprs gtp pdp-context** command is issued while a session handoff is in progress.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)T4f.

Unreproducible Caveat

The following Cisco LTE SPGW caveat has not been reproduced in Cisco IOS Release 12.4(24)T4f.

- CSCty00356

The Cisco LTE SPGW might crash during a 3G-to-4G session handoff.

This condition is observed on the rare occasion that a session cleanup occurs during a 3G-to-4G handoff.

Caveats - Cisco IOS Release 12.4(24)T4e

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1, Cisco IOS Release 12.4(24)T4e image:

- Open Caveats, page 97
- Resolved Caveats, page 99

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 97
- Cisco SAMI Open Caveats, page 99

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4e.

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx62235

  After the charging gateway removes flow control for a session, the Cisco LTE SPGW sends a different GTP message in the middle of the one that was flow-controlled and then continues with the remainder of the GTP message that it was sending previously.

  Workaround: There is currently no known workaround.

- CSCtx91844

  The “S1/X2 change counter” does not increment in the **show gprs gtp statistics** command output after a handover.

  This condition is seen with the following scenario:

  a. S1 with no SGW change.
  b. S1 with an SGW change.
  c. X2 with no SGW change.
  d. X2 with an SGW change.

Additionally, the S1 and X2 counters are calculated incorrectly; therefore, they are not serving the purpose for which they are intended. The S1 and X2 counters generate incorrect information while debugging as well.

Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCtx94762

  Spurious memory tracebacks are observed when deleting the sessions after a GTPv1-to-GTPv2 handoff.

  The spurious memory tracebacks occur due to an unrealistic scenario (signaling with “error indications” in the modify bearer request) in landslide and is observed when downlink traffic is received when a GTPv1-to-GTPv2 handoff is in progress.

  Workaround: There is currently no known workaround.

- CSCtx94845

  After a pre-Release 8 SGSN-to-S4 SGSN handover, the Cisco LTE SPGW retains the pre-Release 8 SGSN path, even after all the sessions are removed.

  This condition occurs when the switchover occurs before the old SGSN path is removed due to a path cleanup timer expiration after a GTPv1-to-GTPv2 handover on the active gateway.

  Workaround: There is currently no known workaround.

- CSCty00356

  The Cisco LTE SPGW might crash during a 3G-to-4G session handoff.

  This condition is observed on the rare occasion that a session cleanup occurs during a 3G-to-4G handoff.

  Workaround: There is currently no known workaround.

- CSCty03462

  The Cisco LTE SPGW detects a Public Land Mobile Network (PLMN) change during a 3G-to-4G or 4G-to-3G handoff, and sets the PLMN ID change bit in the change condition for the service container.

  This condition occurs with an inter-routing access technology handoff.

  Workaround: There is currently no known workaround.

- CSCty55350

  When an IPv6 subscriber user disconnects and attempts to reconnect, an error message is seen on the reconnect attempt. This error message is seen only when the IPv6 MTU is great than 1432.

  Workaround: Configure the IPv6 MTU to a value lesser than or equal to 1432.

- CSCtx93599

The Cisco LTE SPGW closes a P-CDR with a value of 24 before a switchover or with a value of 18 after a switchover during a PGW-to-SPGW mode change as part of an S1-base handover.

This condition happens on the newly active gateway if an SPGW switchover occurs before a final modify bearer request comes to the SPGW to complete the S1-based handover.

Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4e.

- 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 occasion 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.

- CSCtw60222

  The following hardware failure notice is seen on the LCP side:

  ```
  %SAMI-3-730205: SAMI User Space: ERROR: Proc-3 hw watchdog timeout event received
  %SAMI-3-730205: SAMI User Space: ERROR: lcp handle ppc crash notice for proc 3
  %SAMI-5-730203: SAMI User Space: Notice: Reload reason: Proc 3 - hw watchdog failure
  ```

  No specific conditions appear to trigger the failure notice; however, any process that has disabled interrupts for more than 3 seconds appears to trigger the failure notice.

  Workaround: There is currently no known workaround.

- CSCtx85422

  One of 56 lookup threads in the IXP micro engine fails to process packets. There are no specific symptoms of this condition because syslogs are not generated and the other 55 threads are capable of handling packets. Additionally, this condition does not cause any noticeable degradation in performance.

  This condition occurs because one of the lookup threads fails to initialize properly and fails to receive packets.

  Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4e. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 99
- Cisco SAMI Resolved Caveats, page 102

Cisco LTE SPGW Resolved Caveats

This section lists SPGW-specific caveats that are resolved in Cisco IOS Release 12.4(24)T4e.

- CSCtx58888

The **show gprs gtp status** command output displays an incorrect value for the "Postpaid PDPs" counter:

```
SPGW# show gprs gtp status
...
Service-aware Status:
  Prepaid PDPs                          0
  Postpaid PDPs                         4294966417
...
```

This condition is seen when there is a failover and a standby gateway becomes the active gateway.

- CSCtx86993

  For IPv6 UE, after Radio Access Bearer (RAB), packets should be buffered at approximately 20 packets per second (pps). Instead, Cisco Express Forwarding (CEF) code is dropping packets at a much higher rate; hence the packet buffering behavior is not 20 packets pps.

- CSCtx97871

  The following SYSLOG is observed during the switchover:

  ```
  SAMI 3/4: Feb 14 11:42:56.149: %PLATFORM-3-UNFORESEEN: Free PDP already sent for index
  (303491).
  ```

  There is no operational impact due to this SYSLOG message, which occurs if there are some PDPs in a deleting state because of a restart count change and there is a switchover. The SYSLOG is printed on the newly active gateway.

- CSCtx00520

  The **show ipv6 local pool** command output displays a positive value for the "inuse count" field even though there are no active IPv6 sessions (GTPv1 and GTPv2).

  This condition is seen when a create-on-create request or delete-on-create request for an IPv6 session occurs when the following configuration exists:

  a. No multipools are configured with the same IPv6 pool name.
  b. The first range of the pool does not have a parent. For example, the parent pool does not have a parent.

- CSCtx67355

  Incorrect counter when packets are dropped due to buffering on the gateway after the maximum buffer packet limit is reached. Packets are punted from Cisco Express Forwarding (CEF) to process even after buffer limit is reached.

  This condition occurs when buffering on the gateway is enabled.

- CSCtx95132

  The Cisco LTE SPGW generates an SGW-CDR for a session for which 3G-to-4G handoff is not complete and a switchover occurs twice. Because the handoff is not complete, the SPGW should not open an SGW-CDR; therefore, it is incorrect behavior that the SPGW creates an SGW-CDR when the Mobility Management Entity (MME) sends the create session request for a handoff to 4G. A modify bearer request is not sent to complete the handoff.

  This condition occurs went the gateway reloads two times while a session is in the preparatory phase of a GTPv1-toGTPv2 handoff.

- CSCty00582

  A new data path on the standby gateway with Radio Network Controller (RNC) is shown as an SGSN interface instead of an RNC interface with direct tunnel support is enabled.

This condition occurs when a direct tunnel is established for the PDP.

- CSCty00618

  The Cisco LTE SPGW might reload when it comes up as a standby gateway. This reload occurs during the “standby cold buck” to “standby hot” transition while the sychronization of sessions from the active is occurring.

  For this reload to occur, there has to be a session on the active gateway that is in one of the following state, which is a part of the bulk sync to the standby gateway:

  - iRAT is occurring for the session (v1->SP) and the handover is not yet complete.
  - The session is undergoing an internally triggered deletion (such as idle timeout).
  - The session is waiting for usage from the CSG2 when the bulk sync occurs.

- CSCty00880

  When a create session request is received for the same session during a 4G-to-3G handover, and the gateway is waiting for Service Control Usage (SCU), spurious memory access is seen.

  The 4G session comes up properly; however a message indicating spurious memory access is written to the console.

  This condition exists when the gateway is waiting for SCU for the session during a 4G-to-3G handoff when the create session request arrives.

- CSCty03897

  Currently, when a PowerPC (PPC) crash due to a BUS error occurs, the PPC does not store the address access that caused the BUS error.

  This condition occurs when there is a machine check exception.

- CSCty25906

  The Cisco LTE SPGW generates a different control plane Fully Qualified Tunnel End Point Identifier (FTEID) for sessions of same user during a 3G-to-4G handover of these sessions.

  This condition occurs if there are multiple 3G PDN connections for the same user and the sessions are handed over to 4G. When this occurs, the SPGW responds with different control plane FTEIDs in the create session responses to the target mobility management entity (MME).

- CSCty31400

  Sessions are deleted and recreated with the following syslog message:

  ```
  %LTE_GTPV2-4-LTE_RESTART_COUNTER_CHANGED: GSN: 2606:AE00:2001:B00::3, Sig src addr:
  167::11, TID: 0705420121517054, MME: 167::11 Restart counter changed from 52 to 56,
  reason: LTE Path restart counter changed
  ```

  This condition occurs when performing mode change for a session and the restart counter information element (IE) difference for Mobility Management Entity (MME) and the Serving Gateway (SGW) is less than 32. The sessions are deleted and recreated.

- CSCty34806

  The Cisco LTE SPGW reloads might reload when multiple successful and failed handoffs occur.

  This reload occurs only with the following scenario:

  a. Two GTPv1 PDP contexts (session 1 and session 2) are created.
  b. A GTPv1-to-GTPv2 handoff request is sent for session 2.
  c. Session 2 is handed back to GTPv1.
  d. A QoS update for session 1 is sent.

e. An update request with SGSN change is sent. (This request should be rejected due to system failure.)

f. A GTPv1-to-GTPv2 handoff for session 1 is initiated. (This handoff should fail due to no resource available and the session remains a GTPv1 session.

g. A new GTPv2 create session request with a different restart value is sent.

- CSCty37716

  Sometimes, the MTU configuration under Virtual-Template is not saved to the startup config. This condition occurs only if 1500 is the configured MTU. For LTE, separate MTUs are required for IPv4 and IPv6. These MTUs can be configured and saved correctly.

Cisco SAMI Resolved Caveats

This section lists SAMI-specific caveats that are resolved with Cisco IOS Release 12.4(24)T4e.

- CSCty03443

  The Cisco SAMI reloads due to an IXP health monitoring failure and the following system log message is seen on the PowerPC (PPC) console.

  ```
  %PLATFORM-1-DP_HM_FAIL: Failed to receive response from IXP1.
  ```

  Check the health monitor configuration (configured by using the **sami health-monitoring** command in global configuration mode) and issue the **show sami health-monitoring** command in privileged EXEC mode for more information.

  This condition occurs when a null buffer handle is processed by the data path in the IXP micro engine. Each packet processed has an associated buffer handle. A null buffer handle is invalid and when processed by IXP, fails to respond to health monitoring messages from the PPCs.

- CSCty22416

  If a Machine Check Exception (MCE) occurs for any of the PowerPCs (PPCs), the Cisco SAMI might reload without creating a crashinfo file. All reloads due to an MCE do not create a crashinfo file.

- CSCty26519

  If a downstream IPv4 packet has the Don't Fragment (DF) bit set and after adding the tunnel header, the packet exceeds the egress VLAN MTU, the packet will be CEF-switched instead of MEF.

  This condition occurs when the downstream IPv4 packet has the DF bet set and after adding the tunnel header, the packet exceeds the egress VLAN MTU.

Caveats - Cisco IOS Release 12.4(24)T4d

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2.1, Cisco IOS Release 12.4(24)T4d image:

- Open Caveats, page 103
- Resolved Caveats, page 106

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 103
- Cisco SAMI Open Caveats, page 105

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4d.

- CSCtw57615

  The Cisco LTE SPGW reaches high CPU usage due to IP input process when more than 400 Mbps downlink data traffic is being continuously sent over a single user session, which also has data buffering and no S1-U path established.

  This high CPU usage occurs when the following conditions exist:

  a. Downstream data for one user is received at a rate of 400Mbps when S1-U path is not established.

  b. Even after sending a Downlink Data Notification (DDN) message, the modify bearer request is not received for multiple iterations and the S1-U is never established.

  c. The downlink data keeps on coming at the same rate.

  Workaround: There is currently no known workaround.

- CSCtx00520

  The **show ipv6 local pool** command output displays a positive value for the “inuse count” field even though there are no active IPv6 sessions (GTPv1 and GTPv2).

  This condition is seen when a create-on-create request or delete-on-create request for an IPv6 session occurs when the following configuration exists:

  a. No multipools are configured with the same IPv6 pool name.

  b. The first range of the pool does not have a parent. For example, the parent pool does not have a parent.

  Workaround: Disable the cache entry by setting it to 0 as seen in the following example:

  ```
  ipv6 local pool v6_pool_64K_1 2004:11:100::/48 64 cache-size 0
  ```

- CSCtx56288

  An SNMP poll on cGtpPathRemoteNode returns an incorrect node type. The SNMP poll should return the eNodeB value.

  This condition occurs when there are two paths on the SPGW; one to the Mobile Management Entity (MME) and the other to the eNodeB.

  Workaround: There is currently no known workaround.

- CSCtx58888

  The **show gprs gtp status** command output displays an incorrect value for the “Postpaid PDPs” counter:

```
SPGW# show gprs gtp status
...
Service-aware Status:
  Prepaid PDPs                          0
  Postpaid PDPs                         4294966417
...
```

This condition is seen when there is a failover and a standby gateway becomes the active gateway.

Workaround: There is currently no known workaround.

- CSCtx91844

  The "S1/X2 change counter" does not increment in the **show gprs gtp statistics** command output after a handover.

  This condition is seen with the following scenario:

  a. S1 with no SGW change.

  b. S1 with an SGW change.

  c. X2 with no SGW change.

  d. X2 with an SGW change.

  Additionally, the S1 and X2 counters are calculated incorrectly; therefore, they are not serving the purpose for which they are intended. The S1 and X2 counters generate incorrect information while debugging as well.

  Workaround: There is currently no known workaround.

- CSCtx93599

  The Cisco LTE SPGW closes a P-CDR with a value of 24 before a switchover or with a value of 18 after a switchover during a PGW-to-SPGW mode change as part of an S1-base handover.

  This condition happens on the newly active gateway if an SPGW switchover occurs before a final modify bearer request comes to the SPGW to complete the S1-based handover.

  Workaround: There is currently no known workaround.

- CSCtx94033

  When a session is in SPGW mode and in a deleting state, and a new create session request is received, the SPGW sends a positive create session response back to the Mobility Management Entity (MME). After the session is deleted in the SPGW, no session is created for the user; therefore, there is a mismatch between the MME and SPGW.

  This condition occurs when the session is in SPGW mode and a new create session request is received for an already existing session that is in a deleting state.

  Workaround: Send the new create session request after the session is deleted.

- CSCtx94762

  Spurious memory tracebacks are observed when deleting the sessions after a GTPv1-to-GTPv2 handoff. The spurious memory tracebacks occur due to an unrealistic scenario (signaling with "error indications" in the modify bearer request) in landslide and is observed when downlink traffic is received when a GTPv1-to-GTPv2 handoff is in progress.

  Workaround: There is currently no known workaround.

- CSCtx94845

  After a pre-Release 8 SGSN-to-S4 SGSN handover, the Cisco LTE SPGW retains the pre-Release 8 SGSN path, even after all the sessions are removed.

This condition occurs when the switchover occurs before the old SGSN path is removed due to a path cleanup timer expiration after a GTPv1-to-GTPv2 handover on the active gateway.

Workaround: There is currently no known workaround.

- CSCtx95132

  The Cisco LTE SPGW generates an SGW-CDR for a session for which 3G-to-4G handoff is not complete and a switchover occurs twice. Because the handoff is not complete, the SPGW should not open an SGW-CDR; therefore, it is incorrect behavior that the SPGW creates an SGW-CDR when the Mobility Management Entity (MME) sends the create session request for a handoff to 4G. A modify bearer request is not sent to complete the handoff.

  This condition occurs went the gateway reloads two times while a session is in the preparatory phase of a GTPv1-toGTPv2 handoff.

  Workaround: There is currently no known workaround.

- CSCtx97871

  The following SYSLOG is observed during the switchover:

  ```
  SAMI 3/4: Feb 14 11:42:56.149: %PLATFORM-3-UNFORESEEN: Free PDP already sent for index
  (303491).
  ```

  There is no operational impact due to this SYSLOG message, which occurs if there are some PDPs in a deleting state because of a restart count change and there is a switchover. The SYSLOG is printed on the newly active gateway.

  Workaround: There is currently no known workaround.

- CSCty00356

  The Cisco LTE SPGW might crash during a 3G-to-4G session handoff.

  This condition is observed on the rare occasion that a session cleanup occurs during a 3G-to-4G handoff.

  Workaround: There is currently no known workaround.

- CSCty03462

  The Cisco LTE SPGW detects a Public Land Mobile Network (PLMN) change during a 3G-to-4G or 4G-to-3G handoff, and sets the PLMN ID change bit in the change condition for the service container.

  This condition occurs with an inter-routing access technology handoff.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4d.

- 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 occasion 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.

- CSCtx85422

One of the IXP hardware threads in the Cisco SAMI micro-engine that runs look-up micro-block stop processing packets.

This condition occurs when the receive (rx) micro-block is initialized after the look-up micro-block.

Workaround: There is currently no known workaround.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4d. Only severity 1 and 2 caveats and select severity 3 caveats are listed

- Cisco LTE SPGW Resolved Caveats, page 106
- Cisco SAMI Resolved Caveats, page 110
- Miscellaneous Resolved Caveats, page 110

Cisco LTE SPGW Resolved Caveats

This section lists SPGW-specific caveats that are resolved in Cisco IOS Release 12.4(24)T4d.

- CSCtr74989

  After the SPGW sends the requested modify bearer response, the value of the “rcvd bytes” counter and Mobile Express Forwarding (MEF) “uplink bytes” counter is different. The value for the rcvd bytes counter is more than the value for the MEF uplink bytes counter.

  With a P-CDR, this condition might occur because of a CDR closure due to size limit or service record limit. With an SGW-CDR, this condition might occur because of a CDR closure due to size limit or traffic volume container limit.

- CSCts57635

  The SGSN limit trigger from newly active SPGW is not working correctly.

  This condition occurs with the following sequence of events:

  a. The SGSN change limit is set to 2 and SGSN_1 sends a GTPv1 create request.
  b. SGSN_2 sends an update request.
  c. The current active SPGW is reloaded.
  d. SGSN_3 sends an update request to the newly active SPGW.

  Since two SGSN changes have occurred, the newly active SPGW should close the associated call detail record (CDR), but it does not. Additionally, note that after the SGSN_2 sent an update request (Step b), the SGSN_1 is removed from the SGSN list from the old standby, now newly active SPGW.

- CSCts25037

  After a GTPv2-to-GTPv1 handoff, the **show gprs gtp status** command displays counters with incorrect values. Specifically, the counters display very high values even though there are only a few sessions.

  This condition occurs with the following sequence of events:

  a. Approximately 10,000 GTPv2 sessions are created.
  b. A GTPv2-to-GTPv1 handoff occurs.
  c. While the handoff is occurring, the **clear gprs gtp pdp-context all** command is issued.

  This issue is seen, when a GTPv1 handoff is received for a GTPv2 PDP that is in middle of a delete PDP request.

- CSCts38033

  After approximately eight hours of traffic, with 2.4M 3G PDP contexts running UDP traffic and a 4G capacity test performing 1000 creates and deletes per second, the SPGW crashes.

- CSCtt26090

  The Cisco LTE SPGW crashes while testing a 4G session with IPv6 UE and IPv4 transport. This condition occurs when there were a few IPv6 UE SPGW mode sessions and a few IPv4 UE SGW-only mode sessions over IPv4 transport.

- CSCtt40582

  As designed, the PGW CDR (P-CDR) contains two service records with corresponding data and QoS information, however, the SGW CDR (S-CDR) contains two containers with the first container having 0 bytes of traffic.

  This condition occurs with the following sequence of events:

  a. A GTPv2 session is created.
  b. Data traffic is sent through the session.
  c. A Re-Auth-Request (RAR) message is sent from Policy Control and Charging Rules Function (PCRF) with new APN Aggregate Maximum Bit Rate (APN-AMBR) for the session and it is accepted.
  d. The PGW closes a service record and the SGW closes a container.
  e. Traffic is sent through the session once again and the session is deleted.

- CSCtt43678

  Unable to reuse the same aggregate IPv6 prefix for an APN. The **aggregate ipv6** command configuration under the APN is missing.

  This condition occurs with the following sequence of events:

  a. The **aggregate ipv6** command is configured under the APN.
  b. The **show running-config** command displays the **aggregate ipv6** command configuration under the APN.
  c. The APN is removed and reconfigured using the same IPv6 prefix again.
  d. The **show running-config** command does not display the **aggregate ipv6** command configuration under the APN.

- CSCtt46952

  Cisco CSG2 load balancing is not working properly when two aggregate routes with the same range are configured.

  This condition occurs with the following sequence of events:

  a. Two CSG2 groups and two aggregate routes of the same range (16 addresses) are configured under an APN.
  b. A GTPv1 create request for an MS address that falls in the first subnet aggregate is received and CSG2 group 1 is selected.
  c. A second GTPv1 create request for an MS address that falls in the second subnet aggregate is received and CSG2 group 1 is selected when CSG2 group 2 should be selected instead.

- CSCtw61184

  During a 4G-to-3G handoff, the gateway crashes when Downlink Data Notification (DDN) message timer expires.

This condition occurs when the Cisco LTE SPGW does not receive a Downlink Data Notification (DDN) Ack from the Mobility Management Entity (MME).

- CSCtx11154

  The Cisco IOS software counters are not incremented for the SNMP objects (under the APN MIB) that are listed below:

  - cgprsAccPtMsDeactivatedPdps
  - cgprsAccPtIpv6MsDeactivatedPdps
  - cgprsAccPtv4v6MsDeactivatedPdps
  - cgprsAccPtGgsnDeactivatedPdps
  - cgprsAccPtIpv6GgsnDeactivatedPdps

- CSCtx24021

  Sending data traffic while a 4G-to-3G handoff is in progress causes the Cisco LTE SPGW to crash.

  This condition occurs with the rare scenario of a race condition when data traffic is being switched during a 4G-to-3G handoff.

- CSCtx42736

  When policing is enabled on the Cisco LTE SPGW, a memory leak is seen when the gateway is servicing an SGW-only mode session.

  312 bytes of memory is leaked for chunk “LTE policing r.”

  This condition occurs when policing is configured and the gateway is serving an SGW-only mode session.

- CSCtx45202

  A spurious memory access is made in the Cisco LTE SPGW during the retransmission of a GTPv2 signaling packet after a handoff to a GTPv1 session.

- CSCtx47051

  A memory leak related to an IPv6 router advertisement (RA) is seen in the Cisco LTE SPGW.

  This leak occurs when the S1-U is blocked and the IPv6 RA is not handled as designed. 992 bytes of memory is leaked per message.

- CSCtx48043

  During rare condition when sessions are manually cleared in a standby Cisco LTE SPGW, the standby SPGW crashes.

- CSCtx48530

  A memory leak is sent in the “LTE CB Context” on the standby SPGW.

  This condition occurs while syncing the event of a closing CDR to a standby gateway and the PDP data structures in the standby gateway are not properly handled. 1264 bytes of memory is leaked per synchronization event.

- CSCtx51977

  The Cisco LTE SPGW crashes due to corruption in the accounting session table.

- CSCtx55735

  The Cisco LTE SPGW crashes when handling an modify bearer request response after processing a delete session request.

  This condition occurs when the delete session request releases PDP-related parameters.

- CSCtx72778

  A memory leak seen in the LTE GTP MCB (184 bytes) and PGW MCB context (88 bytes).

  This condition occurs with a 3G-to-4G (in SPGW mode) handoff of a session.

- CSCtx78126

  A traceback occurs during the deletion of PDPs when there is heavy traffic as well.

  This condition occurs with IXP reports of an invalid PDP index on a modify request.

- CSCtx79511

  The active SPGW runs out of IDs because they are leaked. The IDs are leaked during a failed GTPv1 session creation.

- CSCtx79641

  The standby SPGW crashes during the synchronization of 3G IPv6 sessions.

- CSCtx79643

  The Cisco LTE SPGW crashes during an X2-based handoff from an SPGW-to-PGW mode session.

  This condition occurs when there are multiple switchovers when the handoff is in progress.

- CSCtx83645

  The Cisco LTE SPGW crashes when it fails to allocate memory and accesses illegal memory instead.

  This condition occurs when SPGW memory is very low and memory allocation fails.

- CSCtx83795

  The Cisco LTE SPGW crashes due to the memory corruption of the master list.

  This crash occurs when GTPv1-to-SPGW mode handoff is in progress and the session is cleared on SPGW.

- CSCtx86137

  The traffic volume container is not included in the S-CDR during a 4G-to-3G handoff.

- CSCtx88067

  A traceback with spurious memory access seen in the active SPGW during a 4G-to-3G handover.

- CSCtx88454

  A memory leak is observed on the Cisco LTE gateway.

  This leak occurs with a SPGW-initiated update request for a GTPv1 PDP and a response in which a GTPv1 Finite State Machine (FSM) parameter is allocated but not freed after processing. 72 bytes of memory is leaked per this type of response.

- CSCtx89241

  Unable to create a PGW-only mode session when an incorrect remote data path address is received in the CSR.

- CSCtx90948

  A memory leak is seen in the Cisco LTE gateway.

  This condition occurs with an SGW-only mode PDP if the CSR contains the PCO IE while parsing memory is allocated to store that information. Upon freeing the PDP, the allocated memory is not freed. A memory leak of 254 bytes is seen for every session.

- CSCtx91170

An S-CDR has a null PDP type, served PDP address, and Mobile Station International Subscriber Directory Number (msisdn) after a SPGW-to-PGW mode handoff.

- CSCtx95421

  A traceback occurs during GTPv1-to-PGW-only mode handoff. With GTPv1-to-PGW-only mode, there are no SGW structures; therefore, accessing session structures causes the issue.

- CSCtx97997

  The Cisco LTE SPGW crashes while it is closing a CDR during continuous handoff from 3G-to-4G and vice versa. After many such iterations the SPGW reloads while closing the CDR.

Cisco SAMI Resolved Caveats

This section lists SAMI-specific caveats that are resolved with Cisco IOS Release 12.4(24)T4d.

- 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 Plane 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.

- 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.

- CSCtx88394

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

Miscellaneous Resolved Caveats

This section lists miscellaneous caveats that are resolved in Cisco IOS Release 12.4(24)T4d.

- CSCti46171

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

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

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

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

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

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

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

- CSCtr49064

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

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

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

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

- CSCtr91106

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

  This advisory is available at the following link:

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

- CSCts38429

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

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

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

Caveats - Cisco IOS Release 12.4(24)T4c

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.2, Cisco IOS Release 12.4(24)T4c image:

- Open Caveats, page 112

- Resolved Caveats, page 115

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 112
- Cisco SAMI Open Caveats, page 114

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4c.

- CSCtr74989

  After the SPGW sends the requested modify bearer request, the value of the "rcvd bytes" counter and Mobile Express Forwarding (MEF) "uplink bytes" counter is different. The rcvd bytes are more than the MEF uplink bytes.

  This condition occurs with the following sequence of events:

  a. A session is created.
  b. Downlink data packets are sent and counters increment properly.
  c. The SPGW sends request modify bearer request.
  d. Downlink data packets are sent and the counters become inconsistent.

  Workaround: There is currently no known workaround.

- CSCts57635

  The SGSN limit trigger from newly active SPGW is not working correctly.

  This condition occurs with the following sequence of events:

  a. The SGSN change limit is set to 2 and SGSN_1 sends a GTPv1 create request.
  b. SGSN_2 sends an update request.
  c. The current active SPGW is reloaded.
  d. SGSN_3 sends an update request to the newly active SPGW.

  Since two SGSN changes have occurred, the newly active SPGW should close the associated call detail record (CDR), but it does not. Additionally, note that after the SGSN_2 sent an update request (Step b), the SGSN_1 is removed from the SGSN list from the old standby, now newly active SPGW.

  Workaround: There is currently no known workaround.

- CSCts25037

  After a GTPv2-to-GTPv1 handoff, the **show gprs gtp status** command displays counters with incorrect values. Specifically, the counters display very high values even though there are only a few sessions.

  This condition occurs with the following sequence of events:

  a. Approximately 10,000 GTPv2 sessions are created.

b. A GTPv2-to-GTPv1 handoff occurs.

c. While the handoff is occurring, the **clear gprs gtp pdp-context all** command is issued.

This issue is seen, when a GTPv1 handoff is received for a GTPv2 PDP that is in middle of a delete PDP request.

Workaround: There is currently no known workaround.

- CSCts38033

  After approximately eight hours of traffic, with 2.4M 3G PDP contexts running UDP traffic and a 4G capacity test performing 1000 creates and deletes per second, the SPGW crashes.

  Workaround: There is currently no known workaround.

- CSCts40437

  The “tableid” is not updated properly during an SPGW handoff. Specifically, the path is not updated correctly with the available tableid.

  This condition occurs when a create request with VRF-enabled in PGW-only mode, and the session is handed off to SPGW mode.

  Workaround: There is currently no known workaround.

- CSCtt10576

  A high CPU is seen on the Proxy Control Processor (PCOP).

  This condition occurs with a bulk of route add requests. When a session is created, the PCOP adds the route entry for the session. This issue is seen with 25,000 create requests, which subsequently add 25,000 route entries.

  Workaround: There is currently no known workaround.

- CSCtt26090

  The Cisco LTE SPGW crashes while when testing a 4G session with IPv6 UE and IPv4 transport. This condition occurs when there were a few IPv6 UE SPGW mode sessions and a few IPv4 UE SGW-only mode sessions over IPv4 transport.

  Workaround: There is currently no known workaround.

- CSCtt33605

  The received byte count is more than the sent byte count for fragmented data. This condition occurs with the following sequence of events:

  a. Cisco Express Forwarding (CEF) is enabled to check the fragmentation of upstream and downstream data.

  b. Approximately 1500 bytes of downstream data is sent from the packet data network (PDN).

  Workaround: There is currently no known workaround.

- CSCtt40582

  As designed, the PGW CDR (P-CDR) contains two service records with corresponding data and QoS information, however, the SGW CDR (S-CDR) contains two containers with the first container having 0 bytes of traffic.

  This condition occurs with the following sequence of events:

  a. A GTPv2 session is created.

  b. Data traffic is sent through the session.

c. A Re-Auth-Request (RAR) message is sent from Policy Control and Charging Rules Function (PCRF) with new APN Aggregate Maximum Bit Rate (APN-AMBR) for the session and it is accepted.

d. The PGW closes a service record and the SGW closes a container.

e. Traffic is sent through the session once again and the session is deleted.

Workaround: There is currently no known workaround.

- CSCtt43678

  Unable to reuse the same aggregate IPv6 prefix for an APN. The **aggregate ipv6** command configuration under the APN is missing.

  This condition occurs with the following sequence of events:

  a. The **aggregate ipv6** command is configured under the APN.

  b. The **show running-config** command displays the **aggregate ipv6** command configuration under the APN.

  c. The APN is removed and reconfigured using the same IPv6 prefix again.

  d. The **show running-config** command does not display the **aggregate ipv6** command configuration under the APN.

  Workaround: There is currently no known workaround.

- CSCtt46952

  Cisco CSG2 load balancing is not working properly when two aggregate routes with the same range are configured.

  This condition occurs with the following sequence of events:

  a. Two CSG2 groups and two aggregate routes of the same range (16 addresses) are configured under an APN.

  b. A GTPv1 create request for an MS address that falls in the first subnet aggregate is received and CSG2 group 1 is selected.

  c. A second GTPv1 create request for an MS address that falls in the second subnet aggregate is received and CSG2 group 1 is selected when CSG2 group 2 should be selected instead.

  Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveat that is open with Cisco IOS Release 12.4(24)T4c.

- 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 occasion 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.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4c. Only severity 1 and 2 caveats and select severity 3 caveats are listed

- Cisco LTE SPGW Resolved Caveats, page 115
- Cisco SAMI Resolved Caveats, page 115

Cisco LTE SPGW Resolved Caveats

This section lists SPGW-specific caveats that are resolved in Cisco IOS Release 12.4(24)T4c.

- CSCtq98447

  With Cisco Express Forwarding (CEF) switching, the Cisco LTE SPGW drops GTPv1 and GTPv2 traffic when the packet size is greater than 1600 bytes.

  This condition occurs when the configured maximum transmission unit (MTU) size is larger than 1600 bytes from the source device to the SPGW and IP traffic is sent through the SPGW with a packet size greater than 1600 bytes.

- CSCtr47216 (duplicate of CSCtr9369)

  The Cisco LTE SPGW might encounter a “No Open CDR” error message during periods of stress conditions.

  This message was seen under the following conditions:

  1. Approximately 50,000 GTPv1 sessions are created.
  2. Continuous upstream data is sent along with SGSN change updates.
  3. The **clear gprs gtp pdp-context all** command is issued on the SPGW.

  As the PDP contexts are deleted, the following message appears:

  ```
  SAMI 8/4: Jul  8 09:06:51.655: %GPRSFLTMG-6-GPRS_CHARGING_NO_CDR: TID:
  1100010000048515, PDP Flags:48452090, MCB Flags:0000100B, APN: broadband Failed to add
  Service Record (Volume up 690 octets, Volume down 0 octets, duration 0 seconds, Cause:
  serviceIdledOut(6):), Reason: No Open CDR.,  -Traceback= 0x443D6380z 0x4435DBCCz
  0x4435E464z 0x44354774z 0x44354F84z 0x4598E998z 0x4599209Cz
  ```

- CSCtr49225

  Uplink traffic is dropped for sessions that have an IPv6 address and IPv4 GTP transport.

  This condition occurs only when the GTP transport is IPv4 based.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)T4c.

Caveats - Cisco IOS Release 12.4(24)T4b

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.1, Cisco IOS Release 12.4(24)T4b image:

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

Open Caveats

Note Caveats that are open in the most current release are also open in prior releases.

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

- Cisco LTE SPGW Open Caveats, page 116
- Cisco SAMI Open Caveats, page 117

Cisco LTE SPGW Open Caveats

This section lists the SPGW-specific caveats that are open in Cisco IOS Release 12.4(24)T4b:

- CSCto46982

  Uplink traffic is dropped by the Cisco LTE SPGW when the subscriber is in a virtual routing and forwarding instance (VRF) domain that is different from the global domain and the VRF through which the SPGW and Cisco CSG2 exchange quota server communication.

  If the SPGW and Cisco CSG2 quota server communication is via the global routing domain, this condition occurs for all subscribers in any VRF. If the SPGW and CSG2 quota server communication is via a VRF (for example VRF1), this condition occurs for subscribers that are not communicating via the global routing domain or VRF1.

  Workaround: There is currently no known workaround.

- CSCtq98447

  With Cisco Express Forwarding (CEF) switching, the Cisco LTE SPGW drops GTPv1 and GTPv2 traffic when the packet size is greater than 1600 bytes.

  This condition occurs when the configured maximum transmission unit (MTU) size is larger than 1600 bytes from the source device to the SPGW and IP traffic is sent through the SPGW with a packet size greater than 1600 bytes.

  Workaround: At the SPGW, use the default MTU size of 1500 bytes.

- CSCtr47216

  The Cisco LTE SPGW might encounter a “No Open CDR” error message during periods of stress conditions.

  This message was seen under the following conditions:

  1. Approximately 50,000 GTPv1 sessions are created.
  2. Continuous upstream data is sent along with SGSN change updates.
  3. The **clear gprs gtp pdp-context all** command is issued on the SPGW.

  As the PDP contexts are deleted, the following message appears:

  ```
  SAMI 8/4: Jul  8 09:06:51.655: %GPRSFLTMG-6-GPRS_CHARGING_NO_CDR: TID:
  1100010000048515, PDP Flags:48452090, MCB Flags:0000100B, APN: broadband Failed to add
  Service Record (Volume up 690 octets, Volume down 0 octets, duration 0 seconds, Cause:
  serviceIdledOut(6):), Reason: No Open CDR.,  -Traceback= 0x443D6380z 0x4435DBCCz
  0x4435E464z 0x44354774z 0x44354F84z 0x4598E998z 0x4599209Cz
  ```

  Workaround: There is currently no known workaround.

- CSCtr49225

Uplink traffic is dropped for sessions that have an IPv6 address and IPv4 GTP transport.

This condition occurs only when the GTP transport is IPv4 based.

Workaround: There is currently no known workaround.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)T4b:

- 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 occasion 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.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)T4b. Only severity 1 and 2 caveats and select severity 3 caveats are listed

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

Cisco LTE SPGW Resolved Caveats

There are no newly resolved Cisco LTE SPGW caveats in Cisco IOS Release 12.4(24)T4b.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)T4b.

Caveats - Cisco IOS Release 12.4(24)T4a

This section contains the list of caveats that are open in Cisco LTE SPGW Release 2.0, Cisco IOS Release 12.4(24)T4a. The following sections document possible unexpected behavior and describe only severity 1 and 2 caveats and select severity 3 caveats.

- Cisco LTE SPGW, page 117
- Cisco SAMI, page 117

Cisco LTE SPGW

There are no known open Cisco LTE SPGW caveats in Cisco IOS Release 12.4(24)T4a.

Cisco SAMI

There are no known open Cisco SAMI caveats with Cisco IOS Release 12.4(24)T4a.

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

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

- *Cisco IOS Release 12.4 Mainline Release Notes*

  Documentation > **Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline > Release Notes**

- *Cisco IOS Release 12.4 T Release Notes*

  Documentation > **Cisco IOS Software > Cisco IOS Software Releases 12.4 T > Release Notes**

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on Cisco.com at http://www.cisco.com/support/bugtools.

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

  Documentation > **Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline**

Platform-Specific Documents

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

- *Cisco Service and Application Module for IP User Guide*
- Cisco 7600 series routers documentation:
  - *Cisco 7600 Series Internet Router Installation Guide*
  - *Cisco 7600 Series Internet Router Module Installation Guide*
  - *Cisco 7609 Internet Router Installation Guide*

Cisco 7600 series router documentation is available at:

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM, unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference guide. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference guide list command syntax information. Use each configuration guide with its corresponding command reference. On Cisco.com at:

Documentation > **Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline > Command References**

Documentation > **Cisco IOS Software > Cisco IOS Software Releases 12.4 Mainline > Command References > Configuration Guides**

Note To view a list of MIBs supported by Cisco IOS Release 12.4(24T4f, see the *Cisco LTE SPGW Configuration Guide*.

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