Release Notes for Cisco LTE SPGW Gateway Release 2.3 on the Cisco SAMI, Cisco IOS Software Release 12.4(24)YS

Latest Publication Date: October 28, 2014, Cisco IOS Release 12.4(24)YS10

Previous Publication Date: July 21, 2014, Cisco IOS Release 12.4(24)YS09

This release note describes the requirements, dependencies, and caveats for the Cisco Long Term Evolution (LTE) Serving Gateway/PDN Gateway (SPGW) Release 2.3 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)YS releases, see the "Caveats" section on page 15 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 the *Cross-Platform Release Notes for Cisco IOS Release 12.4* located on Cisco.com and with the *Cisco LTE SPGW Release 2.3 Configuration Guide* and the *Cisco LTE SPGW Release 2.3 Command Reference*.

Contents

This release note includes the following information:

- Cisco LTE SPGW Overview, page 2
- System Requirements, page 4
- MIBs, page 6
- Limitations, Restrictions, and Important Notes, page 6
- New and Changed Information, page 7
- Caveats, page 15
- Related Documentation, page 81

Cisco Systems, Inc.
www.cisco.com

- Obtaining Documentation and Submitting a Service Request, page 82

Cisco LTE SPGW Overview

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

- LTE Evolved Packet Core, page 2
- Cisco LTE SPGW Description, page 2

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:

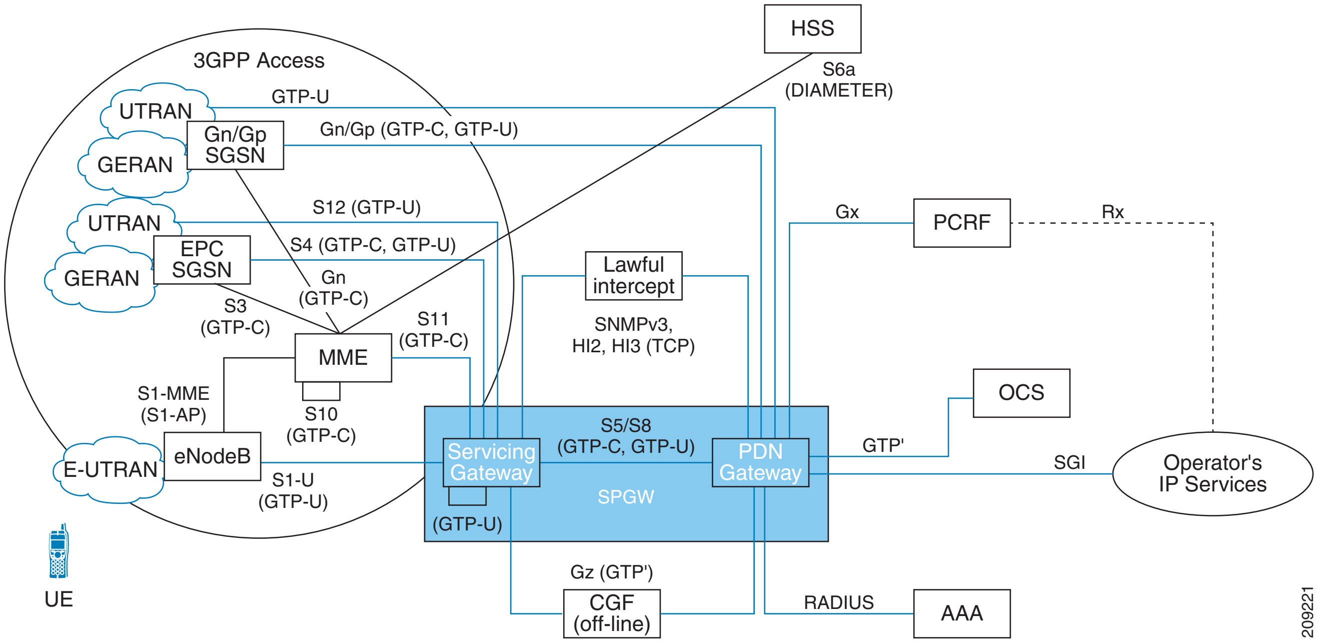
- 4 GB Cisco SAMI, which provides increased session and bearer density

- 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)

Note The Cisco LTE SPGW Release 2.3 supports default bearers only. The Cisco LTE SPGW does not provide dedicated bearer support and with Cisco LTE Release 2.3 and later, gracefully rejects Create Dedicated Bearer requests.

System Requirements

This section describes the system requirements for Cisco LTE SPGW Release 2.*3* and includes the following sections:

- Memory Recommendations, page 4
- Hardware and Software Requirements, page 4
- Determining the Software Version, page 5
- Upgrading to a New Software Release, page 6

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

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco LTE SPGW Release 2.3

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 2.3 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)YS 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. The output displays something similar to the following:

```
SPGW# show version
Cisco IOS Software, SAMI Software (SAMI-L3IK9S-M), Version 12.4(24)YS, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Tue 12-Mar-13 11:59 by prod_rel_team

ROM: System Bootstrap, Version 12.4(20121101:112634)
[buhossai-lte_t4a_cr1812.LTE_R2_V124_24_T4A_THROTTLE_201210300650.19222.ios.sync 101],
DEVELOPMENT SOFTWARE

SGPW uptime is 14 minutes
System returned to ROM by reload at 11:07:22 UTC Wed Mar 13 2013
System restarted at 11:12:43 UTC Wed Mar 13 2013
System image file is "c7svcsami-l3ik9s-mz.124-24.YS.fc2"
```

```
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)YS release, 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 enhancements, documentation corrections and additions have been made:

- The Cisco LTE SPGW Release 2.3 supports default bearers only. The Cisco LTE SPGW does not provide dedicated bearer support and with Cisco LTE Release 2.3 and later, gracefully rejects Create Dedicated Bearer requests.
- The Cisco LTE SPGW Release 2.3 supports dual-stack bearers.
- IPv4 and IPv6 address allocation is performed using locally configured address pools. The Cisco LTE SPGW Release 2.3 does not support DHCP and static IP allocation methods.
- Pre Release 8 QoS Traffic Classes are mapped to Release 8 QoS Class Identifier (QCI) as specified in Table 3:

Table 3 Pre Release 8 Traffic Class to Release 8 QCI Mapping

Traffic Class	QCI	Transfer Delay (in msec)	Signaling Indication	Source Static Descriptor	Traffic Handling Priority
Conversational	1	N/A	N/A	Speech	N/A
Conversational	2	Greater than or equal to 150	N/A	N/A	N/A
Conversational	3	Less than 150	N/A	N/A	N/A
Streaming	4	N/A	N/A	N/A	N/A
Interactive	5	N/A	Yes	N/A	1
Interactive	6	N/A	No	N/A	1
Interactive	7	N/A	N/A	N/A	2
Interactive	8	N/A	N/A	N/A	3
Background	9	N/A	N/A	N/A	N/A

- In Release 8 QoS, all bit rates (MBR and GBR) are counted in bits per second (bps), whereas in pre Release 8 QoS, all bit rates are counted in kilobits per second (kbps). During pre Release 8 -to-Release-8 mapping, bit rates that are received in kbps are converted to bps.
- There is a one-to-one mapping between a Release 8 EPS bearer and pre Release 8 PDP context.

The following section document new features and behavior changes that are introduced in a Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS release. If a Cisco IOS Release 12.4(24)YS 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)YS08

Cisco IOS Release 12.4(24)YS08 introduces the following enhancement and behavior change.

- PGW to accept MBReq without Bearer context in case of ULI, RAT change, page 8

PGW to accept MBReq without Bearer context in case of ULI, RAT change

On S5/S8 interface, when PGW received MBReq without Bearer context in case of ULI and RAT change, PGW rejected the message with conditional IE missing cause code. With Cisco IOS Release 12.2(24)YS08, PGW will not send conditional IE missing cause code. Instead, it will accept this MBR without bearer context.

(CSCun63558)

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YS07

Cisco IOS Release 12.4(24)YS07 introduces the following enhancement and behavior change.

- SCU sanity Check failure counters are not incremented for SCU Sanity failure, page 9

- Adding monitor event logs for unexpected case restart count goes to 0, page 9

SCU sanity Check failure counters are not incremented for SCU Sanity failure

With Cisco IOS Release 12.2(24)YS07, a new counter for the “service record not present” is added in the sync SCU message received from the CSG2. This counter is incremented if the received sync SCU message does not have the service record. This counter is included under **show gprs gtp pdp-context tid <tid> detail** for PDP and **show ggsn csg statistics detailed** for global CSG statistics.

```
Sync Service Control Usage: 1
      No matching req:            0         Processing error:  0
      No service info:            1
```

(CSCum75819)

Adding monitor event logs for unexpected case restart count goes to 0

With Cisco IOS Release 12.2(24)YS07, a new show command, **show monitor event-trace gprs path-debug all**, for path level debugging information is added. This new show command will log information for the condition - path restart count changed from non-zero value to zero. To get output from all TCOPs, use **exec all show monitor event-trace gprs path-debug all**. By default, the debugging logs captured in the **show monitor event-trace gprs path-debug all** will not have the Traceback information. To enable it, the following CLI needs to be configured:

```
Router_B(config)#monitor event-trace gprs path-debug stacktrace
```

Post configuration, existing logs in **show monitor event-trace gprs path-debug all** will be cleared and Traceback information would be seen with newly added debug information logged only with “detail” option in CLI, **show monitor event-trace gprs path-debug all detail.**

(CSCun25893)

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YS06

Cisco IOS Release 12.4(24)YS06 introduces the following enhancement and behavior change.

- GTP Restart Counter - Without Service Internal, page 9
- IPv6 address not fully displayed in all path related output, page 10
- Gtp path counters based on IP address type (v4/v6), page 10
- Adding more registers information to crashinfo for debugging Bus errors, page 10

GTP Restart Counter - Without Service Internal

With Cisco IOS Release 12.2(24)YS06, GTP Own Restart Counter value is included under **show gprs gtp status**. It is independent of "service internal" configuration CLI.

(CSCul49940)

IPv6 address not fully displayed in all path related output

The IPv6 address was not completely displayed for all the below path related show CLI. With Cisco IOS Release 12.2(24)YS06, the IPv6 path is fully displayed (128 bytes):

show gprs gtp path all

show gprs gtp path all detailed

show gprs gtp path statistics remote-address <v4/v6 address>

show gprs gtp path remote-address <v4/v6 address>

show gprs gtp path version

(CSCui76588)

Gtp path counters based on IP address type (v4/v6)

With Cisco IOS Release 12.2(24)YS06, new data path statistics counters were introduced under **show gprs gtp statistics** to display the data (v1) paths created for IP version (v4/v6) and interface (S1u,S4,S5-S8,Gn).

```
V1 data path stats:
 S1u interface
  V4 Created   0            V6 Created     0
 S4 interface
  V4 Created   0            V6 Created     0
 S5-S8 interface
  V4 Created   0
 Gn interface
  V4 Created   0
```

(CSCul83645)

Adding more registers information to crashinfo for debugging Bus errors

To detect Local Bus Controller parity errors and ECM errors, the following registers have been included as part of the crashinfo. It is appended after the PCI bus register information.

```
ECM and Local Bus Controller Registers :
  ECM_EEDR     = 0x00000000 ECM_EEATR     = 0x00000000 ECM_EEADR     = 0x00000000
  LBC_LTESR    = 0x00000000 LBC_LTEATR    = 0x00000000 LBC_LTEAR    = 0x00000000
  LBC_LBCR    = 0x00008000
```

(CSCuj70667)

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YS05

Cisco IOS Release 12.4(24)YS05 introduces the following enhancement and behavior change.

- Collection of available crashinfo during nested exceptions, page 11

Collection of available crashinfo during nested exceptions

In a scenario where a PPC crashes, and collection of crash information begins, the occurrence of a nested exception leads to a state where no crash information is collected for the PPC that crashed.

Before Cisco IOS 12.4(14)YS05, for the SAMI platform, the contents of the RAM is collected and dumped into a single file in the Line Card Processor. The crashed PPC's crash information is collected as part of the bootflash and the RAM dump. Since, in nested exceptions crashinfo collection is disabled, it affects debugging of crashes. In most of the scenarios, second exception was a Bus error and there was very less to debug except the previous reload reason and stack decodes as part of show stacks CLI.

From Cisco IOS 12.4(14)YS05 onwards, during nested exception scenarios, the contents of the RAM is collected and dumped to determine the first exception context. Additionally, Machine check syndrome register value along with the value of the PC, address, and stack decodes of the previous reload is also collected. This helps in debugging machine check exceptions that are hardware-related.

(CSCui87274)

New Implementations and Behavior Changes in Cisco IOS Release 12.4(24)YS02

Cisco IOS Release 12.4(24)YS02 introduces the following enhancements and behavior changes.

- LTE IOS: Increase in data path limit to 16K and total path limit to 32K, page 11
- Error Handling on Path Limits exhausted in SPGW, page 11
- SPGW to support S4-SGSN GTP-U v6 interface, page 12
- ServiceChangeCond field in PGW-CDRs not compliant to 32.298 v8.4.0, page 13
- Restart path is wrongly treated as valid even when restart count is 0, page 13
- Cause Code For DSB session no DSB Flag set or Indication/common flag IE, page 13
- SPGW: Different cause code in V1 and v2 response, page 13
- CSR parsed successfully when there is a mismatch between PDP type and PAA, page 14
- QCI check is not happening at SP-Mode call creation, page 14
- LTE:show command to track ixp usage of network traffic and buffers, page 14
- IXP:Enable parity check on control store, page 15

LTE IOS: Increase in data path limit to 16K and total path limit to 32K

Cisco IOS Release 12.2(24)YS02 has the following enhancements done in SPGW:

- Increased GTP-U path (data path) limit from 8K to 16K.
- Increased total path limit (all versions of GTP-C and GTP-U; and charging) limit from 16K to 32K.

(CSCug79718)

Error Handling on Path Limits exhausted in SPGW

Due to increase in data path limit to 16K and total path limit to 32K with CSCug79718, the DDTS has the below mentioned behavior change:

- GW behavior on reaching Encap ID Table Limit Reached:

  Old behavior:

  Session creation is successful. After 90 seconds (timer), GW detects Data Path Failure due to Encap ID limit and deletes all the sessions on the Path internally. That means, no signaling message indicating deletion to peer nodes. In Case of GGSN (GTPv1) and PGW/SPGW (GTPv2), Accounting Stop is triggered and session is cleared on CSG2/PCEF. Additionally,

  - During the transient 90 second duration (before timer expiry) when the Data Path is without Encap ID, the traffic is Cisco Express Forwarding (CEF) switched.
  - Error indication triggers (sent) and deletion of sessions on receiving error indications works fine.

  New behavior:

  When the path limit is reached due to Encap ID in the GW, it deletes all the sessions in the path internally informing the peer nodes for PGW/SPGW and GGSN modes sessions.

  For S mode, session will be locally deleted without informing the peer.

- GW behavior on reaching CCM or path Handle limit Reached:

  Old behavior:

  On reaching CCM handle limit, session is created successfully and have no mechanism to inform the error from PCOP to TCOP.

  New behavior:

  When the path limit is reached due to CCM handle in the GW, it deletes all the sessions in the path internally informing the peer nodes for PGW/SPGW and GGSN modes sessions.

  For S mode, session will be locally deleted without informing the peer.

With Cisco IOS Release 12.2(24)YS02, a new configuration is introduced to suppress the DBReq and delete the sessions silently on reaching path limit in the GW.

gprs gtp path failure-suppress-dbr

<Sample ..Config...Start>

```
SPGW(config)#gprs gtp path ?
failure-suppress-dbr  Suppress DBReq on path setup failure
history               Specify the history information to be stored
remote                Specify request intervals per peer
SPGW(config)#gprs gtp path
```

<Sample ..Config...End>

(CSCuh09411)

SPGW to support S4-SGSN GTP-U v6 interface

Following enhancement is done in SPGW:

- SPGW to support IPv6 GTP-U interface for S4-SGSN.
- SPGW to send both IPv4 and IPv6 address for S4 GTP-U interface in CSResp and MBResp.
- SPGW will only use IPv6 for S4-SGW GTP-U, if S4-SGSN request has support for both IPv4 and IPv6 address for GTP-U interface.
- SPGW will use IPv6 for S4-SGW GTP-U, if S4-SGSN supports only IPv6 in S4-GTP-U interface.
- SPGW will use IPv4 for S4-SGW GTP-U, if S4-SGSN supports only IPv4 in S4-GTP-U interface.

(CSCug86476)

ServiceChangeCond field in PGW-CDRs not compliant to 32.298 v8.4.0

Before Cisco IOS 12.4(14)YS02, service change condition in service records were updated as bit-string. With Cisco IOS 12.4(14)YS02, service change condition in service records is updated as octet string and bit mask will represent from right to left.

As per 32.298 Specifications, Service change condition needs to update as octet-string instead of bit-string. Also the field is bit mask. For example, SGSN/S-GW and QoS can be changed in the same update request and in the service record, both of these bits will be set. These bit fields has to be updated from LEFT to RIGHT. That means, MSB will be Bit1 and LSB will be Bit 32 and length of the this attribute will be 5 byte.

The current behavior is now in-sync with the Specifications.

(CSCug20647)

Restart path is wrongly treated as valid even when restart count is 0

Before Cisco IOS 12.4(14)YS02, the newly received restart count was treated as valid only if the value is between the range (current_restart_count+1, current_restart_count+32). That means, if the newly received value is y and if it is in range of (x+1, x+32), where x is current path's restart count stored, then the restart count is treated as valid and the path restart count is updated. All other values were treated as invalid.

With Cisco IOS 12.4(14)YS02, the newly received restart count is treated as invalid only if the value is between the range (current_restart_count -32, current_restart_count-1). That means, previous 32 values are invalid and all other values are valid. So the range of the valid values has increased. So if the newly received value is y and if it is in range of (x-32, x-1) where x is current path's restart count stored, then the restart count is treated as invalid. All other values are treated as valid.

(CSCue40849)

Cause Code For DSB session no DSB Flag set or Indication/common flag IE

In the scenario when a DSB CSR containing no Indication IE or DSB flag is not set in the Indication IE (For V2 sessions), and/or with no common Flag IE or DSB flag is not set in the Common Flag (For V1 sessions), are directed towards an IPv4 only or IPV6 only APN, the cause code is mentioned below:

Before Cisco IOS 12.4(14)YS02, for v2 sessions, Returning cause code was 19 (New PDP to single address bearer) and v1 sessions returning cause was 130 (New PDP to single address bearer).

With Cisco IOS 12.4(14)YS02, for v2 call, Returning cause code is 18 (New PDP type due to network preference) and v1 sessions returning cause is 129 (New PDP type due to network preference).

(CSCuf85372)

SPGW: Different cause code in V1 and v2 response

If **create pdp context request** for IPv4 user hits IPv6 APN, then GGSN responds with "Service not supported. (200)".

"Service not supported. (200)" is not the expected cause code as per specification 29.060 for **create pdp context request**. The cause code for this scenario is changed to "system failure".

For v2 sessions, when APN does not support the PDN type, GW sends "system failure" cause. The cause code for this scenario is changed to "Preferred PDN type not supported".

(CSCuh13178)

CSR parsed successfully when there is a mismatch between PDP type and PAA

When there is a mismatch between the PDN type IE (type 99) and PAA IE, the CSRequest should fail in the parsing stage itself and the CSResponse should be rejected with Mandatory IE incorrect. But currently, the GW parses the message successfully and in some cases, the CSRequest is accepted and MS address is allotted to the UE. Even for V1 session, when DSB flag and end user address without DSB is sent in create PDP, the request is accepted.

Cisco IOS Release 12.2(24)YS02 has the following enhancements:

- Removed dual pdntype check in sgw_gtpv2_create_sess_req_sanity_check API.
- Changed the PDNTYPE_IPV4V6 to GTP_PDP_ADDR_TYPE_IPV4V6, because pdn_type has the GTP_PDP_ADDR_TYPE_IPV4V6. The PDNTYPE_IPV4V6 enum value into pdn_type is not stored.

(CSCug09965)

QCI check is not happening at SP-Mode call creation

Create V2 PDP in SP-Mode using GBR values as Qci value. In SP-Mode, we are able to create the session for GBR but in case of SGW and PGW Mode, it is rejected. With Cisco IOS Release 12.2(24)YS02, SP-Mode will reject GBR session.

(CSCue85876)

LTE:show command to track ixp usage of network traffic and buffers

Following four commands is introduced with Cisco IOS 12.4(14)YS02:

show sami ixp network

This command displays the network utilization with respect to output data rate on TX for each IXP in a SAMI card.

show sami ixp network history

This command displays the graphical output of the network utilization for each IXP for the last 60 sec, 60 min and 72 hours.

show sami ixp buffer

This command displays the buffer utilization with respect to 800 pre-allocated DRAM buffers of size 4k for storing incoming packets per IXP.

show sami ixp buffer history

This command displays the graphical output of the buffer utilization for each IXP for the last 60 sec, 60 min and 72 hours.

(CSCuc97902)

IXP:Enable parity check on control store

SAMI (WS-SVC-SAMI-BB-K9) on node AKRNOHCZ91SPG01 was reloaded, as seven contexts (0-6) of PCI ME on IXP-1 stopped responding (thread health monitoring failed). These seven threads

were found to be waiting for signals. Context-0 was waiting for "system startup" signal and contexts 1-6 were waiting for "signal from previous thread" to be triggered by context-0 to start with.

This logic of waiting for signals is only during IXP bootup. When Xscale loads the ucode into ME's, all ME's (threads) do not start processing packets immediately but waits for a signal from RX ME which allocates and initializes all data path related resources (MSF, Q-arrays, Dram buffers, SRAM buffer handles, Free lists and so on). Once RX ME gives "system startup" signal to all the other ME's, threads in those ME's start processing in a tight loop.

Before, exact code location for the Ustore Parity error could not be determined. However, with Cisco IOS 12.4(14)YS02, exact code location for the Ustore Parity error can be determined because Parity detection bit is enabled in all the micro engines.

(CSCud43085)

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 selected 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)YS 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)YS release, on the Bug Toolkit page, use the **Software Version** drop down lists to select Cisco IOS Version 12.4(24)YS 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)YS10, page 16
- Caveats - Cisco IOS Release 12.4(24)YS09, page 18

- Caveats - Cisco IOS Release 12.4(24)YS08a, page 21
- Caveats - Cisco IOS Release 12.4(24)YS08, page 22
- Caveats - Cisco IOS Release 12.4(24)YS07, page 23
- Caveats - Cisco IOS Release 12.4(24)YS06, page 31
- Caveats - Cisco IOS Release 12.4(24)YS05, page 39
- Caveats - Cisco IOS Release 12.4(24)YS04, page 47
- Caveats - Cisco IOS Release 12.4(24)YS03, page 54
- Caveats - Cisco IOS Release 12.4(24)YS02, page 59
- Caveats - Cisco IOS Release 12.4(24)YS01, page 67
- Caveats - Cisco IOS Release 12.4(24)YS, page 74

Caveats - Cisco IOS Release 12.4(24)YS10

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS10 image:

- Open Caveats, page 16
- Resolved Caveats, page 17

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 16
- Cisco SAMI Open Caveats, page 16

Cisco LTE SPGW Open Caveats

There are no newly opened Cisco LTE SPGW specific caveats in Cisco IOS Release 12.4(24)YS10. Refer to "Cisco LTE SPGW Open Caveats" section on page 18, for the list of caveats that are open from prior releases.

Cisco SAMI Open Caveats

This section lists the Cisco SAMI caveats that are open with Cisco IOS Release 12.4(24)YS10.

- CSCtn88798 - Sami got stuck at STDBY COLD after reload

  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 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.

- CSCud36564 - SAMI reloads - PCI MEs 6 threads reported as hanging in an "initialize" state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  Workaround: There is currently no known workaround.

- CSCuh73226 - SAMI Qnx kernel crashes

  SAMI gets reloaded with the reason stating "IXP xscale core received". In the LCP core directory, a file by the name ixp#.txt contains the Qnx kernel core dump.

- CSCum92382 - High usage incorrectly reported in PCDR & SCDR (Fragmented packets).

  1500 byte reassembled Packets from PPC are not sent back to IXP and those reassembled packets are forwarded through PPC (CEF Switched). It causes high volume usage reporting for few users.

  This condition occurs when:

  - Upstream T-PDU packet with 1480 Bytes(data payload) is sent.
  - Downstream packet with 1480 Bytes(data payload) is sent.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)YS10. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 17
- Cisco SAMI Resolved Caveats, page 17

Cisco LTE SPGW Resolved Caveats

The following SPGW caveat is resolved with Cisco IOS Release 12.4(24)YS10.

- CSCur31375 - Reload on receiving spoof pkt when DataPath is idle in foll condition

  Gateway reloads up on receiving spoofed IP packet when data path is idle.

  This condition occurs when data path does not exist with the "**security verify source**" command configured under APN.

- CSCur33535 - Src Addr violation is not happening for V6 users with V6 Data path

  IP Source Addr violation is not applied for IPv6 users when associated with the IPv6 Data path. The "**Src Addr violation**" counter in "**show gprs gtp pdp tid <*tid*>"** CLI output does not get incremented.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI specific caveats in Cisco IOS Release 12.4(24)YS10.

Caveats - Cisco IOS Release 12.4(24)YS09

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS09 image:

- Open Caveats, page 18
- Resolved Caveats, page 20

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 18
- Cisco SAMI Open Caveats, page 20

Cisco LTE SPGW Open Caveats

This section lists the LTE SPGW-specific caveats that are open with Cisco IOS Release 12.4(24)YS09.

- CSCun38527 - Traceback errors causing APN failures

  Traceback with %GPRSFLTMG-3-GPRS_DUP_TID_RADIX_DUP_PDP: Duplicate PDP TID logs

  When an SPGW/PGW mode session is created in Active, failure occurs in Standby after IP address allocation. When the session is deleted in Active and the IP address is allocated to some other session, this condition occurs.

  Workaround: There is currently no known workaround.

- CSCul35268 - Crash at ixp_dp_free_mcb during inter s4-sgsn HO

  Crash is seen at ixp_dp_free_mcb during inter S4-SGSN Handover

  This condition might occur during inter S4-SGSN HO with IPv6 GTP-u interface. When there is path failure on the IPv6 interface, crash could be seen on the Standby Node. The Crash is seen only when there is path failure.

  Workaround: There is currently no known workaround.

- CSCul99805 - SGW sending wrong src IP address, while doing SGW handover

  SGW will respond with a wrong Source IP for CSR response when the session is not present in the PGW, while doing a SGW handover.

  This condition occurs when session is not present in PGW, but its there in MME. At that point of time, when an SGW handover is triggered from MME, SGW will respond CSResponse Context not found with wrong source IP.

  Workaround: There is currently no known workaround.

- CSCuj91502 - YS02 or YS04 - "clear gprs gtp pdp all", not reaching 0

  "clear gprs gtp pdp all" does not clear all the PDP's.

  When SGSN sends Reject cause code for GTPv1, Delete PDP context request is triggered from GW.

Workaround: There is currently no known workaround.

- CSCud77259 - Traceback Observed While Changing Charging port when CDR is buffered

  Spurious memory access in charging function.

  This condition was observed when charging gateway was moved from maintenance to operational with CDRs buffered.

  Workaround: There is currently no known workaround.

- CSCui96836 - R2.3c-GGSN CSG counter showing wrong value

  While checking CLI "**show ggsn csg parameter**", number of session counter was present even though there was no session available on SPGW blade.

  This condition occurs when:

  - GTPv1 session is created for IPv6 users.
  - Clear the session.

  In Standby, the CLI "**show ggsn csg parameter**", number of sessions counters are present after clearing the session.

  Workaround: There is currently no known workaround.

- CSCuj48281 - SAMI User Space: ERROR: Proc 6 - CRASHING (0x00020001) state

  Standby crashed while accessing SGW structure for GGSN mode session.

  This condition occurs when Active has the SGW session and Standby has the GGSN mode session. While synching SGW event from Active to Standby and while updating the SGW structure in Standby, it leads to a crash.

  Workaround: There is currently no known workaround.

- CSCui62793 - Crash at gprs_ho_pdp_upd_handover_cb_p_to_v1

  This condition occurred during V2 (PGW Mode) to V1 handoff.

  Workaround: There is currently no known workaround.

- CSCui65896 - SAMI Crash at gprs_map_chrg_pf_to_chrg_ch

  This condition occurred during MBReq processing in standby.

  Workaround: There is currently no known workaround.

- CSCuh72502 - Gateway crash during un-configure access-point with ipv6 aggregate

  While Ipv6 aggregate list is re-configured under the APN, aggregate list will return freed memory pattern and while removing the APN, Gateway will be crashed.

  This condition occurs when the aggregate list is re-configured in the VRF enabled APN. When an IPv6 aggregate list is added in the VRF enabled APN, it will not take effort as well.

  Workaround: Unconfigure the VRF, then add IPv6 aggregate and configure VRF once again.

- CSCuh84180 - Stale entry seen in the id table

  Stale entry is seen in the encap id table.

  This condition occurs while trying to free the last entity from the table that has exhausted.

  Workaround: There is currently no known workaround.

- CSCug66168 - R2.3:Spurious memory access made@0x9919ACCz reading 0x88

  Spurious memory access is seen while freeing buffer to memory.

This condition occurs when Downlink data packets are sent, datapath is blocked, buffering enabled and enode-b linktype is IPv4.

Workaround: There is currently no known workaround.

- CSCuh80527 - Spurious Memory Access@ixp_dp_modify_mcb During Gamma CM

  Spurious memory access tracebacks is seen on Active SPGW function while doing create-delete-create for V2 PDP.

  Workaround: There is currently no known workaround.

- CSCuh95701 - "Gprs gtp statistics" uplink & Downlink counters showing wrong values.

  "Gprs gtp statistics" Uplink and Downlink counters shows wrong values. There is Access-point statistics packets/bytes counter mismatch.

  This condition occurs while sending traffic.

  Workaround: There is currently no known workaround.

- CSCui01296 - Stale SGSN control paths on Standby while exceeding 32k path limit

  Standby device has stale SGSN control paths while exceeding 32k path limit.

  This condition occurs when new sessions are created after path limit is exhausted in the gateway.

  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)YS09.

- CSCtn88798 - Sami got stuck at STDBY COLD after reload

  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 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.

- CSCud36564 - SAMI reloads - PCI MEs 6 threads reported as hanging in an “initialize” state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  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)YS09. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 20
- Cisco SAMI Resolved Caveats, page 21

Cisco LTE SPGW Resolved Caveats

There are no newly resolved Cisco LTE SPGW specific caveats in Cisco IOS Release 12.4(24)YS09.

Cisco SAMI Resolved Caveats

The following Cisco SAMI-specific caveats are resolved with Cisco IOS Release 12.4(24)YS09.

- CSCuh73226 - SAMI Qnx kernel crashes

  SAMI gets reloaded with the reason stating "IXP xscale core received". In the LCP core directory, a file by the name ixp#.txt contains the Qnx kernel core dump.

- CSCum92382 - High usage incorrectly reported in PCDR & SCDR (Fragmented packets).

  1500 byte reassembled Packets from PPC are not sent back to IXP and those reassembled packets are forwarded through PPC (CEF Switched). It causes high volume usage reporting for few users.

  This condition occurs when:

  - Upstream T-PDU packet with 1480 Bytes(data payload) is sent.
  - Downstream packet with 1480 Bytes(data payload) is sent.

Caveats - Cisco IOS Release 12.4(24)YS08a

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS08a image:

- Open Caveats, page 21
- Resolved Caveats, page 22

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 21
- Cisco SAMI Open Caveats, page 21

Cisco LTE SPGW Open Caveats

There are no newly opened Cisco LTE SPGW specific caveats in Cisco IOS Release 12.4(24)YS08a. Refer to "Cisco LTE SPGW Open Caveats" section on page 23, for the list of caveats that are open from prior releases.

Cisco SAMI Open Caveats

There are no newly opened Cisco SAMI specific caveats in Cisco IOS Release 12.4(24)YS08a. Refer to "Cisco SAMI Open Caveats" section on page 23, for the list of caveats that are open from prior releases.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)YS08a. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 22
- Cisco SAMI Resolved Caveats, page 22

Cisco LTE SPGW Resolved Caveats

The following SPGW caveat is resolved with Cisco IOS Release 12.4(24)YS08a.

- CSCup12309 - Spurious path restarts after the YS08 upgrade

  SPGW detects path restarts incorrectly for GTPv1 paths.

  The condition occurs when there are two GTPv1 messages (Request and Response) pending in the GTP message queue. When the 'Update PDP response' message is processed, instead of retrieving the RIE value from the current response message, the RIE value from the previously processed GTP message is re-used.
- CSCup23009 - Path restart fails for requests with source port other than 2123

  The Recovery IE change or the path restart detection will not happen for SGSN/MME initiated requests.

  This condition occurs if the GTP source port number is not the standard port number, that is 2123.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI specific caveats in Cisco IOS Release 12.4(24)YS08a.

Caveats - Cisco IOS Release 12.4(24)YS08

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS08 image:

- Open Caveats, page 22
- Resolved Caveats, page 23

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 23
- Cisco SAMI Open Caveats, page 23

Cisco LTE SPGW Open Caveats

There are no newly opened Cisco LTE SPGW specific caveats in Cisco IOS Release 12.4(24)YS08. Refer to "Cisco LTE SPGW Open Caveats" section on page 24, for the list of caveats that are open from prior releases.

Cisco SAMI Open Caveats

There are no newly opened Cisco SAMI specific caveats in Cisco IOS Release 12.4(24)YS08. Refer to "Cisco SAMI Open Caveats" section on page 28, for the list of caveats that are open from prior releases.

Resolved Caveats

The following sections list caveats that have been resolved or are unreproducible in Cisco IOS Release 12.4(24)YS08. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 23
- Cisco SAMI Resolved Caveats, page 23

Cisco LTE SPGW Resolved Caveats

There are no newly resolved Cisco LTE SPGW specific caveats in Cisco IOS Release 12.4(24)YS08.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI specific caveats in Cisco IOS Release 12.4(24)YS08.

Caveats - Cisco IOS Release 12.4(24)YS07

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS07 image:

- Open Caveats, page 23
- Resolved Caveats, page 30

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 24
- Cisco SAMI Open Caveats, page 28

Cisco LTE SPGW Open Caveats

This section lists the LTE SPGW-specific caveats that are open with Cisco IOS Release 12.4(24)YS07.

- CSCun38527 - Traceback errors causing APN failures

  Traceback with %GPRSFLTMG-3-GPRS_DUP_TID_RADIX_DUP_PDP: Duplicate PDP TID logs

  When an SPGW/PGW mode session is created in Active, failure occurs in Standby after IP address allocation. When the session is deleted in Active and the IP address is allocated to some other session, this condition occurs.

  Workaround: There is currently no known workaround.

- CSCul35268 - Crash at ixp_dp_free_mcb during inter s4-sgsn HO

  Crash is seen at ixp_dp_free_mcb during inter S4-SGSN Handover

  This condition might occur during inter S4-SGSN HO with IPv6 GTP-u interface. When there is path failure on the IPv6 interface, crash could be seen on the Standby Node. The Crash is seen only when there is path failure.

  Workaround: There is currently no known workaround.

- CSCul39920 - NYCMNYCZ34SPG04-SNMP Process auto restart Detected

  SPGW crashed due to invalid memory reference.

  This invalid memory reference occurred in an error condition and was responsible for SPGW crash while freeing a PDP.

  Workaround: There is currently no known workaround.

- CSCul88007 - Standby SGW crashed when lemon update event syncs

  Standby SAMI Crash.

  Standby SGW crashed while syncing lemon update decode event.

  Workaround: There is currently no known workaround.

- CSCul95498 - Crash at ccm_rf_parse_sync_data

  Standby SPGW crashed while syncing CCM event.

  This condition occurred due to corrupt CCM sync buffer data.

  Workaround: There is currently no known workaround.

- CSCul96286 - SPGW crashed due to memory block corruption

  GW crashed.

  This condition occurred due to corrupt previous and next pointer in the memory block.

  Workaround: There is currently no known workaround.

- CSCul99805 - SGW sending wrong src IP address, while doing SGW handover

  SGW will respond with a wrong Source IP for CSR response when the session is not present in the PGW, while doing a SGW handover.

  This condition occurs when session is not present in PGW, but its there in MME. At that point of time, when an SGW handover is triggered from MME, SGW will respond CSResponse Context not found with wrong source IP.

  Workaround: There is currently no known workaround.

- CSCul81552 - Standby tcop crash while adjacency removal

Standby TCOP crashed while adjacency removal.

This condition occurred while deleting a blocked data path.

Workaround: There is currently no known workaround.

- CSCuj91502 - YS02 or YS04 - "clear gprs gtp pdp all", not reaching 0

  "clear gprs gtp pdp all" does not clear all the PDP's.

  When SGSN sends Reject cause code for GTPv1, Delete PDP context request is triggered from GW.

  Workaround: There is currently no known workaround.

- CSCud77259 - Traceback Observed While Changing Charging port when CDR is buffered

  Spurious memory access in charging function.

  This condition was observed when charging gateway was moved from maintenance to operational with CDRs buffered.

  Workaround: There is currently no known workaround.

- CSCui96836 - R2.3c-GGSN CSG counter showing wrong value

  While checking CLI "**show ggsn csg parameter**", number of session counter was present even though there was no session available on SPGW blade.

  This condition occurs when:

  - GTPv1 session is created for IPv6 users.
  - Clear the session.

  In Standby, the CLI "**show ggsn csg parameter**", number of sessions counters are present after clearing the session.

  Workaround: There is currently no known workaround.

- CSCum16033 - Crash on asn1_encode_serviceRecord

  SPGW Active crashed while handling charging functions.

  This condition occurs while encoding the service record.

  Workaround: There is currently no known workaround.

- CSCum28602 - SAMI reload due to memory outage in TCOP of active node

  CDR buffering caused active TCOP to run out of memory.

  This condition occurs when charging GW or the corresponding interface is down.

  Workaround: There is currently no known workaround.

- CSCuj63032 - SPGW crashed at chunk_remove_sibling(0x990abb4)+0x3c

  During the error scenario, Standby SPGW reloads while freeing the UCB chunk memory.

  This condition occurs when the SPGW syncs Modify Bearer Request to Standby.

  Workaround: There is currently no known workaround.

- CSCuj48281 - SAMI User Space: ERROR: Proc 6 - CRASHING (0x00020001) state

  Standby crashed while accessing SGW structure for GGSN mode session.

  This condition occurs when Active has the SGW session and Standby has the GGSN mode session. While synching SGW event from Active to Standby and while updating the SGW structure in Standby, it leads to a crash.

  Workaround: There is currently no known workaround.

- CSCui91059 - LTE crashes at 'gtp_remove_mcb_framed_routes'

  Standby SPGW crash is observed while processing Delete Session Sync message.

  This condition occurs when stale session is present in the Standby for the same TID.

  Workaround: There is currently no known workaround.
- CSCuj66021 - SAMI SPGW crashed at sgw_bearer_fsm_execute(0x9eb87f0)+0x20c

  Active SGW reloads due to watchdog time-out.

  This condition occurs while receiving Update Bearer Request when waiting for Modify Bearer Response.

  Workaround: There is currently no known workaround.
- CSCui66010 - SNMP: drop counter incr upon gtpv1-c drops from gtp queue

  SPGW should provide the scope of signaling messages dropped from GTP Queue. LTE drop counter (cGtpv2DroppedSigMsgs) currently does this; pre-LTE drop counter does not (cGtpTotalv0v1SigMsgDropped)

  This condition occurs during normal operation.

  Workaround: There is currently no known workaround.
- CSCui83663 - GTP-7-GWDEBUG: PDP:0x1EEB548C, refcnt:1, Wrong refcnt charging_reserved

  SAMI crash reports the following log event and traceback;

  %GTP-7-GWDEBUG: PDP:0x1EEB548C, refcnt:1, Wrong refcnt when charging_reserved, -Traceback= 0x83481C0z 0x8330E74z 0xA28FCB8z 0xA28FEC0z 0x8281BE0z 0x8289440z 0x8289550z 0x8053EECz 0x8054034z 0x82895ACz 0x8290E48z 0x829C284z 0x97BA9A0z 0x97BAAF8z 0x829C410z 0x99DAC6Cz

  ?GTP-7-GWDEBUG: PDP:0x12E2D3A8, refcnt:1, Wrong refcnt when charging_reserved?

  Error message reported during Standby to Active transition.

  Workaround: There is currently no known workaround.
- CSCui19873 - SAMI-SPGW software crash with traceback at gprs_delete_hash_table

  Active SPGW reloads when PDP is deleted upon receiving final SCU for that PDP.

  Workaround: There is currently no known workaround.
- CSCui62793 - Crash at gprs_ho_pdp_upd_handover_cb_p_to_v1

  This condition occurred during V2 (PGW Mode) to V1 handoff.

  Workaround: There is currently no known workaround.
- CSCui65896 - SAMI Crash at gprs_map_chrg_pf_to_chrg_ch

  This condition occurred during MBReq processing in standby.

  Workaround: There is currently no known workaround.
- CSCui66143 - GTPv2-C rcvd counter not incremented in drop case

  This condition occurs whenever the GTPv2-C message is dropped due to GTP Queue exceeding the max limit.

  Workaround: There is currently no known workaround.
- CSCui69837 - SAMI crash during bearer update process

  The standby GW crashed while trying to handle Update bearer response. The crash is because of accessing PDP that is already deleted.

Active will sync the message to Standby GW and then Standby will check whether all the attributes are synced and decoded properly. If any attributes are missed, then it will delete the session. Here, session got deleted and while trying to access deleted session, GW was crashed.

Workaround: There is currently no known workaround.

- CSCui32697 - standby sami crashed, when syncs pdp update process

  Standby reload at lte_sr_decode_and_update

  Active will sync the v1 PDP to Standby GW, but in standby, it will have stale SGW session. GTPv1 sync event on an S-mode PDP, which can lead to a crash.

  Workaround: There is currently no known workaround.

- CSCuh72502 - Gateway crash during un-configure access-point with ipv6 aggregate

  While Ipv6 aggregate list is re-configured under the APN, aggregate list will return freed memory pattern and while removing the APN, Gateway will be crashed.

  This condition occurs when the aggregate list is re-configured in the VRF enabled APN. When an IPv6 aggregate list is added in the VRF enabled APN, it will not take effort as well.

  Workaround: Unconfigure the VRF, then add IPv6 aggregate and configure VRF once again.

- CSCuc00137 - Spurious memory access @ pgw_sm_is_ixp_update_required

  Traceback seen with reading NULL pointer.

  This is seen on active GW during MBR request processing SCU timer expired and reading NULL

  pointer leads the trace-back.

  Workaround: There is currently no known workaround.

- CSCuh16043 - MD's cannot be provisioned after multiple switchover

  MD's cannot be provisioned after multiple switchover

  If any failure occurs during de-provisioning, then it will lead to stale entry in Active and Standby.

  It could also lead stale in LI server. If we try to do LI provisioning after reload Active, it will fail.

  More Information:

  1) Provision 2 MD's, one for IRI and another for CC.

  2) Reload the active, standby takes over as active.

  3) De-Provision the MD's on the current active i.e initial standby.

  4) Run SNMP walk command and no output is shown.

  5) Now reload the current active i.e initial standby and Initial Active takes over as active again.

  6) Now run SNMP walk and no output should be seen and MD's can be provisioned again. But SNMP walk will give some output because of stale entries in GW. So, GW will not allow further provisioning.

  Workaround: There is currently no known workaround.

- CSCuh84180 - Stale entry seen in the id table

  Stale entry is seen in the encap id table.

  This condition occurs while trying to free the last entity from the table that has exhausted.

  Workaround: There is currently no known workaround.

- CSCuh22397 - Reload of SAMI triggered by crash in PDP Update process

  SAMI blade reloaded causing a crashinfo file. The traceback is new type.

This condition occurred during normal operation.

Workaround: There is currently no known workaround.

- CSCug60236 - R2.3:TB:Uninitialized interface pointer-Uninitialized interface pointer

  The syslog seen in Spurious memory access and NULL IDB is given below:

  SAMI 2/6: 010355: Apr 5 12:11:10: %IPV6_FORWARDING-3-NULLIDB: Uninitialized interface pointer - ipv6_fib_forw -Process= "IPv6 Input", ipl= 0, pid= 182, -Traceback= 0x9AC222Cz 0x819F850z 0x8CF39A8z 0x8CF4134z 0x8CF4188z 0x8F4DD44z 0x836984Cz 0x9AC0F2Cz 0x9AC27ACz 0x9AC3AD4z 0x9AB91E8z 0x9ABA1F4z 0x9AC20ECz 0x9AC2468z 0x9ABE6CCz 0x99EEC2Cz

  This condition occurs after clearing the adj. The GW received by the Uplink traffic have seen this traceback.

  Workaround: There is currently no known workaround.

- CSCug66168 - R2.3:Spurious memory access made@0x9919ACCz reading 0x88

  Spurious memory access is seen while freeing buffer to memory.

  This condition occurs when Downlink data packets are sent, datapath is blocked, buffering enabled and enode-b linktype is IPv4.

  Workaround: There is currently no known workaround.

- CSCuh80527 - Spurious Memory Access@ixp_dp_modify_mcb During Gamma CM

  Spurious memory access tracebacks is seen on Active SPGW function while doing create-delete-create for V2 PDP.

  Workaround: There is currently no known workaround.

- CSCuh95701 - "Gprs gtp statistics" uplink & Downlink counters showing wrong values.

  "Gprs gtp statistics" Uplink and Downlink counters shows wrong values. There is Access-point statistics packets/bytes counter mismatch.

  This condition occurs while sending traffic.

  Workaround: There is currently no known workaround.

- CSCui01296 - Stale SGSN control paths on Standby while exceeding 32k path limit

  Standby device has stale SGSN control paths while exceeding 32k path limit.

  This condition occurs when new sessions are created after path limit is exhausted in the gateway.

  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)YS07.

- CSCum92382 - High usage incorrectly reported in PCDR & SCDR (Fragmented packets).

  1500 byte reassembled Packets from PPC are not sent back to IXP and those reassembled packets are forwarded through PPC (CEF Switched). It causes high volume usage reporting for few users.

  This condition occurs when:

  - Upstream T-PDU packet with 1480 Bytes(data payload) is sent.
  - Downstream packet with 1480 Bytes(data payload) is sent.

  Workaround: There is currently no known workaround.

- CSCtn88798 - Sami got stuck at STDBY COLD after reload

  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 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.

- CSCua36249 - Xscale shutdown due to QNX crash, reported as UNKNOWN reload reason

  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.

- CSCud36564 - SAMI reloads - PCI MEs 6 threads reported as hanging in an “initialize” state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  Workaround: There is currently no known workaround.

- CSCue53135 - LTE SPGW: Multiple threads in PCI in thread hung state

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 021084: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:2 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021085: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:3 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021086: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:4 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021087: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:5 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021088: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:6 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021089: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:7 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021090: Jan 16 18:16:46: %PLATFORM-0-DP_IXP_PCI_THR_FAIL: IXP:2 PCI
ME, 8 threads hung
```

  These messages are caused by multiple PCI threads in a hung state.

  Workaround: There is currently no known workaround.

- CSCue78169 - LTE HM failure due to abnormal incr. of fragment lock counter in lookup

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 022445: Feb  1 20:10:30: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:1
SAMI 1/3: 022446: Feb  1 20:10:31: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:2
SAMI 1/3: 022447: Feb  1 20:10:32: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:3
SAMI 1/3: 022448: Feb  1 20:10:38: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:1
SAMI 1/3: 022449: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
```

```
num_consecutive_fail:1
SAMI 1/3: 022450: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:2
SAMI 1/3: 022451: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:4 thr:7
num_consecutive_fail:1
SAMI 1/3: 022452: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:2
SAMI 1/3: 022453: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:
```

These messages are caused by an LTE H/M failure caused by an abnormal increment of the fragment lock counter in lookup.

Workaround: There is currently no known workaround.

- CSCue97620 - IXP QM encountered NULL/Invalid buffer handle

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 000246: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/3: 000247: Feb 24 14:52:34:  PLATFORM-1-DP_HM_FAIL  Failed to receive response
from IXP2. Check `sami health-monitoring' configuration and see `show sami
health-monitoring' for more info
SAMI 1/5: 000039: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/8: 000038: Feb 24 14:52:34:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 in 16 retries, system will reboot if it continues to fail receiving
response in another 16 retries (i.e. in the next 256 milliseconds.)</B>
```

  These messages are caused when the Cisco SAMI LTE QM encounters NULL/Invalid buffer handle.

  Workaround: There is currently no known workaround.

- CSCuh73226 - SAMI Qnx kernel crashes

  SAMI gets reloaded with the reason stating "IXP xscale core received". In the LCP core directory, a file by the name ixp#.txt contains the Qnx kernel core dump.

  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)YS07. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 30
- Cisco SAMI Resolved Caveats, page 31

Cisco LTE SPGW Resolved Caveats

The following SPGW caveat is resolved with Cisco IOS Release 12.4(24)YS07.

- CSCum49687 - Inaccurate UserLocationInformation (ULI DATA MISSING ON Gn-S11 handovers)

  Incorrect ULI sent by SPGW to CSG2 in accounting radius messages.

This condition occurs when GTPv2 message with ULI information is received with at least one digit on both MNC and MCC being 0.

- CSCui87864 - ULI decoding issue when both TAI and ECGI is present.

  SPGW/PGW sends ULI with an extra byte '00' to the radius server.

  ULI with extra one byte '00' is encoded in the condition where both the TAI and ECGI has to be encoded in radius AVP for a 4G session.

- CSCum65599 - GW is not treating zero as valid Restart Counter

  GW responds for Echo request with RIE zero.

  When GW receives an Echo request with RIE zero, Echo response will be sent instead of being rejected.

- CSCum57319 - Echo counter is not incrementing under path statistics for failure case

  Counters are not updated for failure cases.

  This condition might occur when Echo request is received by GW with lesser restart counter.

- CSCum29057 - SAMI crashes at pcop after arp timeout

  SAMI crashed when the ARP request from GW to PCEF failed.

  This condition might occur when the following conditions are met:

  a. APN need to be un-configured (no APN cli) (no reload is performed after config change).

  b. ARP request from the GW to CSG2 HSRP Virtual-IP should be failing.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI specific caveats in Cisco IOS Release 12.4(24)YS07.

Caveats - Cisco IOS Release 12.4(24)YS06

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS06 image:

- Open Caveats, page 31
- Resolved Caveats, page 38

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 32
- Cisco SAMI Open Caveats, page 37

Cisco LTE SPGW Open Caveats

This section lists the LTE SPGW-specific caveats that are open with Cisco IOS Release 12.4(24)YS06.

- CSCum57319 - Echo counter is not incrementing under path statistics for failure case

  Counters are not updated for failure cases.

  This condition might occur when Echo request is received by GW with lesser restart counter.

  Workaround: There is currently no known workaround.

- CSCul35268 - Crash at ixp_dp_free_mcb during inter s4-sgsn HO

  Crash is seen at ixp_dp_free_mcb during inter S4-SGSN Handover

  This condition might occur during inter S4-SGSN HO with IPv6 GTP-u interface. When there is path failure on the IPv6 interface, crash could be seen on the Standby Node. The Crash is seen only when there is path failure.

  Workaround: There is currently no known workaround.

- CSCum49687 - Inaccurate UserLocationInformation(ULI DATA MISSING ON Gn-S11 handovers)

  Incorrect ULI sent by SPGW to CSG2 in accounting radius messages.

  This condition occurs when GTPv2 message with ULI information is received with at least one digit on both MNC and MCC being 0.

  Workaround: There is currently no known workaround.

- CSCul39920 - NYCMNYCZ34SPG04-SNMP Process auto restart Detected

  SPGW crashed due to invalid memory reference.

  This invalid memory reference occurred in an error condition and was responsible for SPGW crash while freeing a PDP.

  Workaround: There is currently no known workaround.

- CSCul88007 - Standby SGW crashed when lemon update event syncs

  Standby SAMI Crash.

  Standby SGW crashed while syncing lemon update decode event.

  Workaround: There is currently no known workaround.

- CSCul95498 - Crash at ccm_rf_parse_sync_data

  Standby SPGW crashed while syncing CCM event.

  This condition occurred due to corrupt CCM sync buffer data.

  Workaround: There is currently no known workaround.

- CSCul96286 - SPGW crashed due to memory block corruption

  GW crashed.

  This condition occurred due to corrupt previous and next pointer in the memory block.

  Workaround: There is currently no known workaround.

- CSCul99805 - SGW sending wrong src IP address, while doing SGW handover

  SGW will respond with a wrong Source IP for CSR response when the session is not present in the PGW, while doing a SGW handover.

This condition occurs when session is not present in PGW, but its there in MME. At that point of time, when an SGW handover is triggered from MME, SGW will respond CSResponse Context not found with wrong source IP.

Workaround: There is currently no known workaround.

- CSCul81552 - Standby tcop crash while adjacency removal

  Standby TCOP crashed while adjacency removal.

  This condition occurred while deleting a blocked data path.

  Workaround: There is currently no known workaround.

- CSCuj91502 - YS02 or YS04 - "clear gprs gtp pdp all", not reaching 0

  "clear gprs gtp pdp all" does not clear all the PDP's.

  When SGSN sends Reject cause code for GTPv1, Delete PDP context request is triggered from GW.

  Workaround: There is currently no known workaround.

- CSCud77259 - Traceback Observed While Changing Charging port when CDR is buffered

  Spurious memory access in charging function.

  This condition was observed when charging gateway was moved from maintenance to operational with CDRs buffered.

  Workaround: There is currently no known workaround.

- CSCui96836 - R2.3c-GGSN CSG counter showing wrong value

  While checking CLI "**show ggsn csg parameter**", number of session counter was present even though there was no session available on SPGW blade.

  This condition occurs when:

  – GTPv1 session is created for IPv6 users.

  – Clear the session.

  In Standby, the CLI "**show ggsn csg parameter**", number of sessions counters are present after clearing the session.

  Workaround: There is currently no known workaround.

- CSCum16033 - Crash on asn1_encode_serviceRecord

  SPGW Active crashed while handling charging functions.

  This condition occurs while encoding the service record.

  Workaround: There is currently no known workaround.

- CSCum28602 - SAMI reload due to memory outage in TCOP of active node

  CDR buffering caused active TCOP to run out of memory.

  This condition occurs when charging GW or the corresponding interface is down.

  Workaround: There is currently no known workaround.

- CSCum29057 - SAMI crashes at pcop after arp timeout

  SAMI crashed when the ARP request from GW to PCEF failed.

  This condition might occur when the following conditions are met:

  a. APN need to be un-configured (no APN cli) (no reload is performed after config change).

  b. ARP request from the GW to CSG2 HSRP Virtual-IP should be failing.

Workaround: There is currently no known workaround.

- CSCuj63032 - SPGW crashed at chunk_remove_sibling(0x990abb4)+0x3c

  During the error scenario, Standby SPGW reloads while freeing the UCB chunk memory.

  This condition occurs when the SPGW syncs Modify Bearer Request to Standby.

  Workaround: There is currently no known workaround.

- CSCuj48281 - SAMI User Space: ERROR: Proc 6 - CRASHING (0x00020001) state

  Standby crashed while accessing SGW structure for GGSN mode session.

  This condition occurs when Active has the SGW session and Standby has the GGSN mode session. While synching SGW event from Active to Standby and while updating the SGW structure in Standby, it leads to a crash.

  Workaround: There is currently no known workaround.

- CSCui91059 - LTE crashes at 'gtp_remove_mcb_framed_routes'

  Standby SPGW crash is observed while processing Delete Session Sync message.

  This condition occurs when stale session is present in the Standby for the same TID.

  Workaround: There is currently no known workaround.

- CSCuj66021 - SAMI SPGW crashed at sgw_bearer_fsm_execute(0x9eb87f0)+0x20c

  Active SGW reloads due to watchdog time-out.

  This condition occurs while receiving Update Bearer Request when waiting for Modify Bearer Response.

  Workaround: There is currently no known workaround.

- CSCui66010 - SNMP: drop counter incr upon gtpv1-c drops from gtp queue

  SPGW should provide the scope of signaling messages dropped from GTP Queue. LTE drop counter (cGtpv2DroppedSigMsgs) currently does this; pre-LTE drop counter does not (cGtpTotalv0v1SigMsgDropped)

  This condition occurs during normal operation.

  Workaround: There is currently no known workaround.

- CSCui83663 - GTP-7-GWDEBUG: PDP:0x1EEB548C, refcnt:1, Wrong refcnt charging_reserved

  SAMI crash reports the following log event and traceback;

  %GTP-7-GWDEBUG: PDP:0x1EEB548C, refcnt:1, Wrong refcnt when charging_reserved, -Traceback= 0x83481C0z 0x8330E74z 0xA28FCB8z 0xA28FEC0z 0x8281BE0z 0x8289440z 0x8289550z 0x8053EECz 0x8054034z 0x82895ACz 0x8290E48z 0x829C284z 0x97BA9A0z 0x97BAAF8z 0x829C410z 0x99DAC6Cz

  ?GTP-7-GWDEBUG: PDP:0x12E2D3A8, refcnt:1, Wrong refcnt when charging_reserved?

  Error message reported during Standby to Active transition.

  Workaround: There is currently no known workaround.

- CSCui19873 - SAMI-SPGW software crash with traceback at gprs_delete_hash_table

  Active SPGW reloads when PDP is deleted upon receiving final SCU for that PDP.

  Workaround: There is currently no known workaround.

- CSCui62793 - Crash at gprs_ho_pdp_upd_handover_cb_p_to_v1

  This condition occurred during V2 (PGW Mode) to V1 handoff.

Workaround: There is currently no known workaround.

- CSCui65896 - SAMI Crash at gprs_map_chrg_pf_to_chrg_ch

  This condition occurred during MBReq processing in standby.

  Workaround: There is currently no known workaround.

- CSCui66143 - GTPv2-C rcvd counter not incremented in drop case

  This condition occurs whenever the GTPv2-C message is dropped due to GTP Queue exceeding the max limit.

  Workaround: There is currently no known workaround.

- CSCui69837 - SAMI crash during bearer update process

  The standby GW crashed while trying to handle Update bearer response. The crash is because of accessing PDP that is already deleted.

  Active will sync the message to Standby GW and then Standby will check whether all the attributes are synced and decoded properly. If any attributes are missed, then it will delete the session. Here, session got deleted and while trying to access deleted session, GW was crashed.

  Workaround: There is currently no known workaround.

- CSCui32697 - standby sami crashed, when syncs pdp update process

  Standby reload at lte_sr_decode_and_update

  Active will sync the v1 PDP to Standby GW, but in standby, it will have stale SGW session. GTPv1 sync event on an S-mode PDP, which can lead to a crash.

  Workaround: There is currently no known workaround.

- CSCuh72502 - Gateway crash during un-configure access-point with ipv6 aggregate

  While Ipv6 aggregate list is re-configured under the APN, aggregate list will return freed memory pattern and while removing the APN, Gateway will be crashed.

  This condition occurs when the aggregate list is re-configured in the VRF enabled APN. When an IPv6 aggregate list is added in the VRF enabled APN, it will not take effort as well.

  Workaround: Unconfigure the VRF, then add IPv6 aggregate and configure VRF once again.

- CSCuc00137 - Spurious memory access @ pgw_sm_is_ixp_update_required

  Traceback seen with reading NULL pointer.

  This is seen on active GW during MBR request processing SCU timer expired and reading NULL

  pointer leads the trace-back.

  Workaround: There is currently no known workaround.

- CSCuh16043 - MD's cannot be provisioned after multiple switchover

  MD's cannot be provisioned after multiple switchover

  If any failure occurs during de-provisioning, then it will lead to stale entry in Active and Standby.

  It could also lead stale in LI server. If we try to do LI provisioning after reload Active, it will fail.

  More Information:

  1) Provision 2 MD's, one for IRI and another for CC.

  2) Reload the active, standby takes over as active.

  3) De-Provision the MD's on the current active i.e initial standby.

  4) Run SNMP walk command and no output is shown.

5) Now reload the current active i.e initial standby and Initial Active takes over as active again.

6) Now run SNMP walk and no output should be seen and MD's can be provisioned again. But SNMP walk will give some output because of stale entries in GW. So, GW will not allow further provisioning.

Workaround: There is currently no known workaround.

- CSCuh84180 - Stale entry seen in the id table

  Stale entry is seen in the encap id table.

  This condition occurs while trying to free the last entity from the table that has exhausted.

  Workaround: There is currently no known workaround.

- CSCuh22397 - Reload of SAMI triggered by crash in PDP Update process

  SAMI blade reloaded causing a crashinfo file. The traceback is new type.

  This condition occurred during normal operation.

  Workaround: There is currently no known workaround.

- CSCug60236 - R2.3:TB:Uninitialized interface pointer-Uninitialized interface pointer

  The syslog seen in Spurious memory access and NULL IDB is given below:

  SAMI 2/6: 010355: Apr 5 12:11:10: %IPV6_FORWARDING-3-NULLIDB: Uninitialized interface pointer - ipv6_fib_forw -Process= "IPv6 Input", ipl= 0, pid= 182, -Traceback= 0x9AC222Cz 0x819F850z 0x8CF39A8z 0x8CF4134z 0x8CF4188z 0x8F4DD44z 0x836984Cz 0x9AC0F2Cz 0x9AC27ACz 0x9AC3AD4z 0x9AB91E8z 0x9ABA1F4z 0x9AC20ECz 0x9AC2468z 0x9ABE6CCz 0x99EEC2Cz

  This condition occurs after clearing the adj. The GW received by the Uplink traffic have seen this traceback.

  Workaround: There is currently no known workaround.

- CSCug66168 - R2.3:Spurious memory access made@0x9919ACCz reading 0x88

  Spurious memory access is seen while freeing buffer to memory.

  This condition occurs when Downlink data packets are sent, datapath is blocked, buffering enabled and enode-b linktype is IPv4.

  Workaround: There is currently no known workaround.

- CSCuh80527 - Spurious Memory Access@ixp_dp_modify_mcb During Gamma CM

  Spurious memory access tracebacks is seen on Active SPGW function while doing create-delete-create for V2 PDP.

  Workaround: There is currently no known workaround.

- CSCuh95701 - "Gprs gtp statistics" uplink & Downlink counters showing wrong values.

  "Gprs gtp statistics" Uplink and Downlink counters shows wrong values. There is Access-point statistics packets/bytes counter mismatch.

  This condition occurs while sending traffic.

  Workaround: There is currently no known workaround.

- CSCui01296 - Stale SGSN control paths on Standby while exceeding 32k path limit

  Standby device has stale SGSN control paths while exceeding 32k path limit.

  This condition occurs when new sessions are created after path limit is exhausted in the gateway.

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)YS06.

- CSCtn88798 - Sami got stuck at STDBY COLD after reload

  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 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.

- CSCua36249 - Xscale shutdown due to QNX crash, reported as UNKNOWN reload reason

  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.

- CSCud36564 - SAMI reloads - PCI MEs 6 threads reported as hanging in an “initialize” state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  Workaround: There is currently no known workaround.

- CSCue53135 - LTE SPGW: Multiple threads in PCI in thread hung state

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 021084: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:2 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021085: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:3 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021086: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:4 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021087: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:5 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021088: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:6 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021089: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:7 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021090: Jan 16 18:16:46: %PLATFORM-0-DP_IXP_PCI_THR_FAIL: IXP:2 PCI
  ME, 8 threads hung
  ```

  These messages are caused by multiple PCI threads in a hung state.

  Workaround: There is currently no known workaround.

- CSCue78169 - LTE HM failure due to abnormal incr. of fragment lock counter in lookup

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 022445: Feb  1 20:10:30: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:14 thr:5
  num_consecutive_fail:1
  SAMI 1/3: 022446: Feb  1 20:10:31: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:14 thr:5
  num_consecutive_fail:2
  ```

```
SAMI 1/3: 022447: Feb  1 20:10:32: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:3
SAMI 1/3: 022448: Feb  1 20:10:38: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:1
SAMI 1/3: 022449: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:1
SAMI 1/3: 022450: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:2
SAMI 1/3: 022451: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:4 thr:7
num_consecutive_fail:1
SAMI 1/3: 022452: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:2
SAMI 1/3: 022453: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:
```

These messages are caused by an LTE H/M failure caused by an abnormal increment of the fragment lock counter in lookup.

Workaround: There is currently no known workaround.

- CSCue97620 - IXP QM encountered NULL/Invalid buffer handle

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 000246: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/3: 000247: Feb 24 14:52:34:  PLATFORM-1-DP_HM_FAIL  Failed to receive response
from IXP2. Check `sami health-monitoring' configuration and see `show sami
health-monitoring' for more info
SAMI 1/5: 000039: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/8: 000038: Feb 24 14:52:34:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 in 16 retries, system will reboot if it continues to fail receiving
response in another 16 retries (i.e. in the next 256 milliseconds.)</B>
```

  These messages are caused when the Cisco SAMI LTE QM encounters NULL/Invalid buffer handle.

  Workaround: There is currently no known workaround.

- CSCuh73226 - SAMI Qnx kernel crashes

  SAMI gets reloaded with the reason stating "IXP xscale core received". In the LCP core directory, a file by the name ixp#.txt contains the Qnx kernel core dump.

  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)YS06. 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)YS06.

- CSCul24607 - IXP DP path Failure syslogs seen for ipv6 data paths

  IPv6 Path Failure Syslogs are observed on Standby Nodes (For IPv6 Data Paths).

  " %GPRSFLTMG-0-GPRS_SERVICE: GSN: 2606:AE00:2001:700::3, Reason: 1, Path fail from 180::1"

  This syslog is observed when:

  - Initial IPv6 Data Path is created successfully and path is not deleted for 4 Hours (Now Path is on PCOP and one of the TCOPs, for example TCOP1).
  - After 4 Hours, if Path for the same remote node is created on new TCOP, for example TCOP2, Path fail will be observed on TCOP2.
- CSCul24631 - Standby SGW crashed when ixp dp path fail syslogs seen and UBR received

  When syslogs of IXP DP path failure is seen on Standby SGW and if PCRF triggers RAR, Standby SGW may crash.

  SPGWB#

  SAMI 9/4: 000039: Nov 2 00:17:33.063 PDT: %GPRSFLTMG-3-GTP_PATH_SETUP_FAILURE: Signaling/Data path setup failed due to IXP DP path Failure [vrf 0x0] (0.0.0.0 <2152>)

  SAMI 9/4: 000040: Nov 2 00:17:33.063 PDT: %GPRSFLTMG-0-GPRS_SERVICE: GSN:<v6 Address of GW>, Reason: 1, Path fail from <v6 Address of Path>
- CSCuj49576 - ALLNTXCZ92SPG04 reloaded

  Active SPGW crash was observed while accessing freed pointer.

  The active SPGW crashed while switching a buffered data packet, which got freed during a error scenario. The switching of buffered data packet was triggered by a MBR which established the S1-u data path.
- CSCuj30029 - Invalid access of freed pdp after an error scenario of decode failure

  Standby SPGW crashed.

  This condition occurred due to UBRsp sync failure on standby GW PDP is posted for deletion. While wrongly referencing data structure of this PDP leads to crash.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI specific caveats in Cisco IOS Release 12.4(24)YS06.

Caveats - Cisco IOS Release 12.4(24)YS05

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS05 image:

- Open Caveats, page 40
- Resolved Caveats, page 45

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 40
- Cisco SAMI Open Caveats, page 43

Cisco LTE SPGW Open Caveats

This section lists the LTE SPGW-specific caveats that are open with Cisco IOS Release 12.4(24)YS05.

- CSCuj63032 - SPGW crashed at chunk_remove_sibling(0x990abb4)+0x3c

  During the error scenario, Standby SPGW reloads while freeing the UCB chunk memory.

  This condition occurs when the SPGW syncs Modify Bearer Request to Standby.

  Workaround: There is currently no known workaround.
- CSCuj48281 - SAMI User Space: ERROR: Proc 6 - CRASHING (0x00020001) state

  Standby crashed while accessing SGW structure for GGSN mode session.

  This condition occurs when Active has the SGW session and Standby has the GGSN mode session. While synching SGW event from Active to Standby and while updating the SGW structure in Standby, it leads to a crash.

  Workaround: There is currently no known workaround.
- CSCui91059 - LTE crashes at 'gtp_remove_mcb_framed_routes'

  Standby SPGW crash is observed while processing Delete Session Sync message.

  This condition occurs when stale session is present in the Standby for the same TID.

  Workaround: There is currently no known workaround.
- CSCuj49576 - ALLNTXCZ92SPG04 reloaded

  Active SPGW crash was observed while accessing freed pointer.

  The active SPGW crashed while switching a buffered data packet, which got freed during a error scenario. The switching of buffered data packet was triggered by a MBR which established the S1-u data path.

  Workaround: There is currently no known workaround.
- CSCuj66021 - SAMI SPGW crashed at sgw_bearer_fsm_execute(0x9eb87f0)+0x20c

  Active SGW reloads due to watchdog time-out.

  This condition occurs while receiving Update Bearer Request when waiting for Modify Bearer Response.

  Workaround: There is currently no known workaround.
- CSCui66010 - SNMP: drop counter incr upon gtpv1-c drops from gtp queue

SPGW should provide the scope of signaling messages dropped from GTP Queue. LTE drop counter (cGtpv2DroppedSigMsgs) currently does this; pre-LTE drop counter does not (cGtpTotalv0v1SigMsgDropped)

This condition occurs during normal operation.

Workaround: There is currently no known workaround.

- CSCui83663 - GTP-7-GWDEBUG: PDP:0x1EEB548C, refcnt:1, Wrong refcnt charging_reserved

  SAMI crash reports the following log event and traceback;

  %GTP-7-GWDEBUG: PDP:0x1EEB548C, refcnt:1, Wrong refcnt when charging_reserved, -Traceback= 0x83481C0z 0x8330E74z 0xA28FCB8z 0xA28FEC0z 0x8281BE0z 0x8289440z 0x8289550z 0x8053EECz 0x8054034z 0x82895ACz 0x8290E48z 0x829C284z 0x97BA9A0z 0x97BAAF8z 0x829C410z 0x99DAC6Cz

  ?GTP-7-GWDEBUG: PDP:0x12E2D3A8, refcnt:1, Wrong refcnt when charging_reserved?

  Error message reported during Standby to Active transition.

  Workaround: There is currently no known workaround.

- CSCui19873 - SAMI-SPGW software crash with traceback at gprs_delete_hash_table

  Active SPGW reloads when PDP is deleted upon receiving final SCU for that PDP.

  Workaround: There is currently no known workaround.

- CSCui62793 - Crash at gprs_ho_pdp_upd_handover_cb_p_to_v1

  This condition occurred during V2 (PGW Mode) to V1 handoff.

  Workaround: There is currently no known workaround.

- CSCui65896 - SAMI Crash at gprs_map_chrg_pf_to_chrg_ch

  This condition occurred during MBReq processing in standby.

  Workaround: There is currently no known workaround.

- CSCui66143 - GTPv2-C rcvd counter not incremented in drop case

  This condition occurs whenever the GTPv2-C message is dropped due to GTP Queue exceeding the max limit.

  Workaround: There is currently no known workaround.

- CSCui69837 - SAMI crash during bearer update process

  The standby GW crashed while trying to handle Update bearer response. The crash is because of accessing PDP that is already deleted.

  Active will sync the message to Standby GW and then Standby will check whether all the attributes are synced and decoded properly. If any attributes are missed, then it will delete the session. Here, session got deleted and while trying to access deleted session, GW was crashed.

  Workaround: There is currently no known workaround.

- CSCui32697 - standby sami crashed, when syncs pdp update process

  Standby reload at lte_sr_decode_and_update

  Active will sync the v1 PDP to Standby GW, but in standby, it will have stale SGW session. GTPv1 sync event on an S-mode PDP, which can lead to a crash.

  Workaround: There is currently no known workaround.

- CSCuh72502 - Gateway crash during un-configure access-point with ipv6 aggregate

While Ipv6 aggregate list is re-configured under the APN, aggregate list will return freed memory pattern and while removing the APN, Gateway will be crashed.

This condition occurs when the aggregate list is re-configured in the VRF enabled APN. When an IPv6 aggregate list is added in the VRF enabled APN, it will not take effort as well.

Workaround: Unconfigure the VRF, then add IPv6 aggregate and configure VRF once again.

- CSCuc00137 - Spurious memory access @ pgw_sm_is_ixp_update_required

  Traceback seen with reading NULL pointer.

  This is seen on active GW during MBR request processing SCU timer expired and reading NULL

  pointer leads the trace-back.

  Workaround: There is currently no known workaround.

- CSCuh16043 - MD's cannot be provisioned after multiple switchover

  MD's cannot be provisioned after multiple switchover

  If any failure occurs during de-provisioning, then it will lead to stale entry in Active and Standby.

  It could also lead stale in LI server. If we try to do LI provisioning after reload Active, it will fail.

  More Information:

  1) Provision 2 MD's, one for IRI and another for CC.

  2) Reload the active, standby takes over as active.

  3) De-Provision the MD's on the current active i.e initial standby.

  4) Run SNMP walk command and no output is shown.

  5) Now reload the current active i.e initial standby and Initial Active takes over as active again.

  6) Now run SNMP walk and no output should be seen and MD's can be provisioned again. But SNMP walk will give some output because of stale entries in GW. So, GW will not allow further provisioning.

  Workaround: There is currently no known workaround.

- CSCuh84180 - Stale entry seen in the id table

  Stale entry is seen in the encap id table.

  This condition occurs while trying to free the last entity from the table that has exhausted.

  Workaround: There is currently no known workaround.

- CSCuh22397 - Reload of SAMI triggered by crash in PDP Update process

  SAMI blade reloaded causing a crashinfo file. The traceback is new type.

  This condition occurred during normal operation.

  Workaround: There is currently no known workaround.

- CSCug60236 - R2.3:TB:Uninitialized interface pointer-Uninitialized interface pointer

  The syslog seen in Spurious memory access and NULL IDB is given below:

  SAMI 2/6: 010355: Apr 5 12:11:10: %IPV6_FORWARDING-3-NULLIDB: Uninitialized interface pointer - ipv6_fib_forw -Process= "IPv6 Input", ipl= 0, pid= 182, -Traceback= 0x9AC222Cz 0x819F850z 0x8CF39A8z 0x8CF4134z 0x8CF4188z 0x8F4DD44z 0x836984Cz 0x9AC0F2Cz 0x9AC27ACz 0x9AC3AD4z 0x9AB91E8z 0x9ABA1F4z 0x9AC20ECz 0x9AC2468z 0x9ABE6CCz 0x99EEC2Cz

This condition occurs after clearing the adj. The GW received by the Uplink traffic have seen this traceback.

Workaround: There is currently no known workaround.

- CSCug66168 - R2.3:Spurious memory access made@0x9919ACCz reading 0x88

  Spurious memory access is seen while freeing buffer to memory.

  This condition occurs when Downlink data packets are sent, datapath is blocked, buffering enabled and enode-b linktype is IPv4.

  Workaround: There is currently no known workaround.

- CSCuh80527 - Spurious Memory Access@ixp_dp_modify_mcb During Gamma CM

  Spurious memory access tracebacks is seen on Active SPGW function while doing create-delete-create for V2 PDP.

  Workaround: There is currently no known workaround.

- CSCuh95701 - "Gprs gtp statistics" uplink & Downlink counters showing wrong values.

  "Gprs gtp statistics" Uplink and Downlink counters shows wrong values. There is Access-point statistics packets/bytes counter mismatch.

  This condition occurs while sending traffic.

  Workaround: There is currently no known workaround.

- CSCui01296 - Stale SGSN control paths on Standby while exceeding 32k path limit

  Standby device has stale SGSN control paths while exceeding 32k path limit.

  This condition occurs when new sessions are created after path limit is exhausted in the gateway.

  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)YS05.

- CSCtn88798 - Sami got stuck at STDBY COLD after reload

  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 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.

- CSCua36249 - Xscale shutdown due to QNX crash, reported as UNKNOWN reload reason

  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.

- CSCud36564 - SAMI reloads - PCI MEs 6 threads reported as hanging in an “initialize” state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  Workaround: There is currently no known workaround.

- CSCue53135 - LTE SPGW: Multiple threads in PCI in thread hung state

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 021084: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:2 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021085: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:3 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021086: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:4 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021087: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:5 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021088: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:6 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021089: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:7 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021090: Jan 16 18:16:46: %PLATFORM-0-DP_IXP_PCI_THR_FAIL: IXP:2 PCI
  ME, 8 threads hung
  ```

  These messages are caused by multiple PCI threads in a hung state.

  Workaround: There is currently no known workaround.

- CSCue78169 - LTE HM failure due to abnormal incr. of fragment lock counter in lookup

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 022445: Feb  1 20:10:30: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:14 thr:5
  num_consecutive_fail:1
  SAMI 1/3: 022446: Feb  1 20:10:31: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:14 thr:5
  num_consecutive_fail:2
  SAMI 1/3: 022447: Feb  1 20:10:32: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:14 thr:5
  num_consecutive_fail:3
  SAMI 1/3: 022448: Feb  1 20:10:38: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:10 thr:0
  num_consecutive_fail:1
  SAMI 1/3: 022449: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:9 thr:4
  num_consecutive_fail:1
  SAMI 1/3: 022450: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:10 thr:0
  num_consecutive_fail:2
  SAMI 1/3: 022451: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:4 thr:7
  num_consecutive_fail:1
  SAMI 1/3: 022452: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:9 thr:4
  num_consecutive_fail:2
  SAMI 1/3: 022453: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:10 thr:0
  num_consecutive_fail:
  ```

  These messages are caused by an LTE H/M failure caused by an abnormal increment of the fragment lock counter in lookup.

  Workaround: There is currently no known workaround.

- CSCue97620 - IXP QM encountered NULL/Invalid buffer handle

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 000246: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/3: 000247: Feb 24 14:52:34:  PLATFORM-1-DP_HM_FAIL  Failed to receive response
from IXP2. Check `sami health-monitoring' configuration and see `show sami
health-monitoring' for more info
SAMI 1/5: 000039: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/8: 000038: Feb 24 14:52:34:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 in 16 retries, system will reboot if it continues to fail receiving
response in another 16 retries (i.e. in the next 256 milliseconds.)</B>
```

These messages are caused when the Cisco SAMI LTE QM encounters NULL/Invalid buffer handle.

Workaround: There is currently no known workaround.

- CSCuh73226 - SAMI Qnx kernel crashes

  SAMI gets reloaded with the reason stating "IXP xscale core received". In the LCP core directory, a file by the name ixp#.txt contains the Qnx kernel core dump.

  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)YS05. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 45
- Cisco SAMI Resolved Caveats, page 46

Cisco LTE SPGW Resolved Caveats

The following SPGW caveat is resolved with Cisco IOS Release 12.4(24)YS05.

- CSCuj83380 - Crash seen when processing DSR

  Active SPGW crashed while processing DSR.

  While clearing huge number of PDPs (in this case 350K PDPs) during upgrade procedure, if deleting S-mode PDP receives DSR with SI and no EBI, and in this flow of event, if a half freed packet pointer is referenced, the code enters an incorrect condition leading to crash while referencing uninitialized pointer.

- CSCui61606 - SNMP: SPGW DDN signaling counter spikes

  SNMP GTPv2 signaling counters (e.g. cGtpv2DownlinkDataNotifs.1 and cGtpv2DownlinkDataNotifAcks.2) report spikes, despite Counter32 behavior is only to increment.

  This condition occurred during normal operation.

- CSCui60516 - SPGWs not sending PGWADDRESS in SCDR

  SAMI SPGWs are intermittently sending a 'NULL' value for the PGWADDRESS field within the SCDR records.

  SAMI configuration has PGW-ADDRESS-USED = ENABLED

  SCDR records sometimes include |-- pGWAddressUsed (6 bytes): field in SCDR and sometimes they do not.

- CSCui81659 - New Data TEID Not updated to MEF when SGSN IP remains same

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

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

- CSCui66000 - syslog for gtpv2-c dropped from gtp queue

  SPGW should notify management system when dropping signaling messages from GTP Queue. Current behavior includes syslog notification for pre-LTE signaling (GTPv0 and GTPv1), but not for LTE signaling (GTPv2).

  This condition occurred during normal operation.

- CSCug94640 - gateway crashed at pgw_send_successful_modify(0x9e63e54)+0x2c8

  The crash is observed when the GW is trying to process the SCU and send Modify Bearer Response.

  This condition occurs when GW is trying to process the SCU and send Modify Bearer Response simultaneously. SCU is received for the PDP and also the delete event is triggered because of an internal event (idle time-out or clear command or path failure etc.).

  In this scenario, if the delete event is processed first then it will go ahead and flush the pending Queue requests and post a delete to the Queue. Now, before processing delete, if there is a context switch and SCU is processed then SCU tries to post a DONE event to Queue. However, since it does not find the corresponding event, accessing invalid memory under PDP structure causes the crash.

- CSCui61940 - Missing LocalSequenceNumber in PGW records

  Duplicate LRSN (Local Record Sequence Number) was observed in PGW records from the same node ID and PGW address. These duplicate LRSN observed from the CDRs generated from different TCOPs in the same SAMI. Same TCOP will not generate this duplicate LRSN.

  From initial analysis, issue can be observed when there are SPGW sessions.

- CSCug93865 - Bearer Qos value is 0 in IRI during 3g-4g Handover

  Bearer Qos value is 0 in IRI during 3G to 4G Handover.

  This condition occurred during 3G to 4G Handover.

  On 3G to 4G Handover, the IRI value should point at the value that is present in new CSR but it points at 0.

- CSCuh88565 - ULI not correctly updated in SGW after S4-S11-S4 HO

  Irregularity in ULI output in SGW, PGW, TID output and CDR.

  This condition occurs when a User performs handoff from S4-S11-S4. When the user finally lands as S4 user, the SGW mode still retains the old ULI but PGW updates itself with new ULI. The CDR's are also generated incorrectly. This happens only in SGW-PGW mode.

- CSCuh83201 - Data Volume Reported in S-CDR does not contain Data After HO

  The Data volume reported in S-CDR and P-CDR do not match and the S-CDR does not account for the data sent after S1 Hand over.

  This condition occurs during S1 Handover. Modify bearer request is received without ULI change or without ULI IE.

Cisco SAMI Resolved Caveats

The following Cisco SAMI-specific caveat is resolved with Cisco IOS Release 12.4(24)YS05.

- CSCuj28610 - IXP uses ipv4 mac address for ipv6 traffic of DSB user

  IPv6 traffic uses IPv4 mac address and sends the traffic in the case DSB.

  This condition is applicable only in the Dual Stack case.

Caveats - Cisco IOS Release 12.4(24)YS04

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS04 image:

- Open Caveats, page 47
- Resolved Caveats, page 53

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 47
- Cisco SAMI Open Caveats, page 51

Cisco LTE SPGW Open Caveats

This section lists the LTE SPGW-specific caveats that are open with Cisco IOS Release 12.4(24)YS04.

- CSCui60516 - SPGWs not sending PGWADDRESS in SCDR

  SAMI SPGWs are intermittently sending a 'NULL' value for the PGWADDRESS field within the SCDR records.

  SAMI configuration has PGW-ADDRESS-USED = ENABLED

  SCDR records sometimes include |-- pGWAddressUsed (6 bytes): field in SCDR and sometimes they do not.

  Workaround: There is currently no known workaround.

- CSCui61606 - SNMP: SPGW DDN signaling counter spikes

  SNMP GTPv2 signaling counters (e.g. cGtpv2DownlinkDataNotifs.1 and cGtpv2DownlinkDataNotifAcks.2) report spikes, despite Counter32 behavior is only to increment.

  This condition occurs during normal operation.

  Workaround: There is currently no known workaround.

- CSCui61940 - Missing LocalSequenceNumber in PGW records

  Duplicate LRSN (Local Record Sequence Number) was observed in PGW records from the same node ID and PGW address. These duplicate LRSN observed from the CDRs generated from different TCOPs in the same SAMI. Same TCOP will not generate this duplicate LRSN.

  From initial analysis, issue can be observed when there are SPGW sessions.

Workaround: There is currently no known workaround.

- CSCui66000 - syslog for gtpv2-c dropped from gtp queue

  SPGW should notify management system when dropping signaling messages from GTP Queue. Current behavior includes syslog notification for pre-LTE signaling (GTPv0 and GTPv1), but not for LTE signaling (GTPv2).

  This condition occurs during normal operation.

  Workaround: There is currently no known workaround.

- CSCui66010 - SNMP: drop counter incr upon gtpv1-c drops from gtp queue

  SPGW should provide the scope of signaling messages dropped from GTP Queue. LTE drop counter (cGtpv2DroppedSigMsgs) currently does this; pre-LTE drop counter does not (cGtpTotalv0v1SigMsgDropped)

  This condition occurs during normal operation.

  Workaround: There is currently no known workaround.

- CSCui83663 - GTP-7-GWDEBUG: PDP:0x1EEB548C, refcnt:1, Wrong refcnt charging_reserved

  SAMI crash reporting the following log event and traceback;

  %GTP-7-GWDEBUG: PDP:0x1EEB548C, refcnt:1, Wrong refcnt when charging_reserved, -Traceback= 0x83481C0z 0x8330E74z 0xA28FCB8z 0xA28FEC0z 0x8281BE0z 0x8289440z 0x8289550z 0x8053EECz 0x8054034z 0x82895ACz 0x8290E48z 0x829C284z 0x97BA9A0z 0x97BAAF8z 0x829C410z 0x99DAC6Cz

  ?GTP-7-GWDEBUG: PDP:0x12E2D3A8, refcnt:1, Wrong refcnt when charging_reserved?

  Error message reported during Standby to Active transition.

  Workaround: There is currently no known workaround.

- CSCui19873 - SAMI-SPGW software crash with traceback at gprs_delete_hash_table

  Active SPGW reloads when PDP is deleted upon receiving final SCU for that PDP.

  Workaround: There is currently no known workaround.

- CSCui62793 - Crash at gprs_ho_pdp_upd_handover_cb_p_to_v1

  This condition occurred during V2 (PGW Mode) to V1 handoff.

  Workaround: There is currently no known workaround.

- CSCui65896 - SAMI Crash at gprs_map_chrg_pf_to_chrg_ch

  This condition occurred during MBReq processing in standby.

  Workaround: There is currently no known workaround.

- CSCui66143 - GTPv2-C rcvd counter not incremented in drop case

  This condition occurs whenever the GTPv2-C message is dropped due to GTP Queue exceeding the max limit.

  Workaround: There is currently no known workaround.

- CSCui69837 - SAMI crash during bearer update process

  The standby GW crashed while trying to handle Update bearer response. The crash is because of accessing PDP that is already deleted.

  Active will sync the message to Standby GW and then standby will check whether all the attributes are synced and decoded properly. If any attributes are missed, then it will delete the session. Here, session got deleted and while trying to access deleted session, GW was crashed.

Workaround: There is currently no known workaround.

- CSCui81659 - New Data TEID Not updated to MEF when SGSN IP remains same

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

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

  Workaround: There is currently no known workaround.

- CSCug94640 - gateway crashed at pgw_send_successful_modify(0x9e63e54)+0x2c8

  The crash is observed when the GW is trying to process the SCU and send Modify Bearer Response.

  This condition occurs when GW is trying to process the SCU and send Modify Bearer Response simultaneously. SCU is received for the PDP and also the delete event is triggered because of an internal event (idle time-out or clear command or path failure etc.).

  In this scenario, if the delete event is processed first then it will go ahead and flush the pending Queue requests and post a delete to the Queue. Now, before processing delete, if there is a context switch and SCU is processed then SCU tries to post a DONE event to Queue. However, since it does not find the corresponding event, accessing invalid memory under PDP structure causes the crash.

  Workaround: There is currently no known workaround.

- CSCui32697 - standby sami crashed, when syncs pdp update process

  Standby reload at lte_sr_decode_and_update

  Active will sync the v1 PDP to Standby GW, but in standby, it will have stale SGW session. GTPv1 sync event on an S-mode PDP, which can lead to a crash.

  Workaround: There is currently no known workaround.

- CSCuh72502 - Gateway crash during un-configure access-point with ipv6 aggregate

  While Ipv6 aggregate list is re-configured under the APN, aggregate list will return freed memory pattern and while removing the APN, Gateway will be crashed.

  This condition occurs when the aggregate list is re-configured in the VRF enabled APN. When an IPv6 aggregate list is added in the VRF enabled APN, it will not take effort as well.

  Workaround: Unconfigure the VRF, then add IPv6 aggregate and configure VRF once again.

- CSCuc00137 - Spurious memory access @ pgw_sm_is_ixp_update_required

  Traceback seen with reading NULL pointer.

  This is seen on active GW during MBR request processing SCU timer expired and reading NULL

  pointer leads the trace-back.

  Workaround: There is currently no known workaround.

- CSCug93865 - Bearer Qos value is 0 in IRI during 3g-4g Handover

  Bearer Qos value is 0 in IRI during 3G to 4G Handover.

  This condition occurs during 3G to 4G Handover.

  On 3G to 4G Handover, the IRI value should point at the value that is present in new CSR but it points at 0.

  Workaround: There is currently no known workaround.

- CSCuh16043 - MD's cannot be provisioned after multiple switchover

  MD's cannot be provisioned after multiple switchover

If any failure happens during de-provisioning, then it will lead to stale entry in active and standby.

It could also lead stale in LI server. If we try to do LI provisioning after reload Active, it will fail.

More Information:

1) Provision 2 MD's, one for IRI and another for CC.

2) Reload the active, standby takes over as active.

3) De-Provision the MD's on the current active i.e initial standby.

4) Run SNMP walk command and no output is shown.

5) Now reload the current active i.e initial standby and Initial Active takes over as active again.

6) Now run SNMP walk and no output should be seen and MD's can be provisioned again. But SNMP

walk will give some output because of stale entries in GW. So, GW will not allow further provisioning.

Workaround: There is currently no known workaround.

- CSCuh83201 - Data Volume Reported in S-CDR does not contain Data After HO

  The Data volume reported in S-CDR and P-CDR do not match and the S-CDR does not account for the data sent after S1 Hand over.

  This condition occurs during S1 Handover. Modify bearer request is received without ULI change or without ULI IE.

  Workaround: There is currently no known workaround.

- CSCuh84180 - Stale entry seen in the id table

  Stale entry is seen in the encap id table.

  This condition occurs while trying to free the last entity from the table that has exhausted.

  Workaround: There is currently no known workaround.

- CSCuh88565 - ULI not correctly updated in SGW after S4-S11-S4 HO

  Irregularity in ULI output in SGW, PGW, TID output and CDR.

  This condition occurs when a User performs handoff from S4-S11-S4. When the user finally lands as S4 user, the SGW mode still retains the old ULI but PGW updates itself with new ULI. The CDR's are also generated incorrectly. This happens only in SGW-PGW mode.

  Workaround: There is currently no known workaround.

- CSCuh22397 - Reload of SAMI triggered by crash in PDP Update process

  SAMI blade reloaded causing a crashinfo file. The traceback is new type.

  This condition occurred during normal operation.

  Workaround: There is currently no known workaround.

- CSCug60236 - R2.3:TB:Uninitialized interface pointer-Uninitialized interface pointer

  The syslog seen in Spurious memory access and NULL IDB is given below:

  SAMI 2/6: 010355: Apr 5 12:11:10: %IPV6_FORWARDING-3-NULLIDB: Uninitialized interface pointer - ipv6_fib_forw -Process= "IPv6 Input", ipl= 0, pid= 182, -Traceback= 0x9AC222Cz 0x819F850z 0x8CF39A8z 0x8CF4134z 0x8CF4188z 0x8F4DD44z 0x836984Cz 0x9AC0F2Cz 0x9AC27ACz 0x9AC3AD4z 0x9AB91E8z 0x9ABA1F4z 0x9AC20ECz 0x9AC2468z 0x9ABE6CCz 0x99EEC2Cz

This condition occurs after clearing the adj. The GW received by the Uplink traffic have seen this traceback.

Workaround: There is currently no known workaround.

- CSCug66168 - R2.3:Spurious memory access made@0x9919ACCz reading 0x88

  Spurious memory access is seen while freeing buffer to memory.

  This condition occurs when Downlink data packets are sent, datapath is blocked, buffering enabled and enode-b linktype is IPv4.

  Workaround: There is currently no known workaround.

- CSCuh80527 - Spurious Memory Access@ixp_dp_modify_mcb During Gamma CM

  Spurious memory access tracebacks is seen on Active SPGW function while doing create-delete-create for V2 PDP.

  Workaround: There is currently no known workaround.

- CSCuh95701 - "Gprs gtp statistics" uplink & Downlink counters showing wrong values.

  "Gprs gtp statistics" Uplink and Downlink counters shows wrong values. There is Access-point statistics packets/bytes counter mismatch.

  This condition occurs while sending traffic.

  Workaround: There is currently no known workaround.

- CSCui01296 - Stale SGSN control paths on Standby while exceeding 32k path limit

  Standby device has stale SGSN control paths while exceeding 32k path limit.

  This condition occurs when new sessions are created after path limit is exhausted in the gateway.

  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)YS04.

- CSCtn88798—Sami got stuck at STDBY COLD after reload

  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 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.

- CSCua36249—Xscale shutdown due to QNX crash, reported as UNKNOWN reload reason

  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.

- CSCud36564—SAMI reloads - PCI MEs 6 threads reported as hanging in an “initialize” state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  Workaround: There is currently no known workaround.

- CSCue53135—LTE SPGW: Multiple threads in PCI in thread hung state

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 021084: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:2 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021085: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:3 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021086: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:4 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021087: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:5 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021088: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:6 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021089: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:7 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021090: Jan 16 18:16:46: %PLATFORM-0-DP_IXP_PCI_THR_FAIL: IXP:2 PCI
  ME, 8 threads hung
  ```

  These messages are caused by multiple PCI threads in a hung state.

  Workaround: There is currently no known workaround.

- CSCue78169—LTE HM failure due to abnormal incr. of fragment lock counter in lookup

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 022445: Feb  1 20:10:30: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:14 thr:5
  num_consecutive_fail:1
  SAMI 1/3: 022446: Feb  1 20:10:31: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:14 thr:5
  num_consecutive_fail:2
  SAMI 1/3: 022447: Feb  1 20:10:32: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:14 thr:5
  num_consecutive_fail:3
  SAMI 1/3: 022448: Feb  1 20:10:38: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:10 thr:0
  num_consecutive_fail:1
  SAMI 1/3: 022449: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:9 thr:4
  num_consecutive_fail:1
  SAMI 1/3: 022450: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:10 thr:0
  num_consecutive_fail:2
  SAMI 1/3: 022451: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:4 thr:7
  num_consecutive_fail:1
  SAMI 1/3: 022452: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:9 thr:4
  num_consecutive_fail:2
  SAMI 1/3: 022453: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:10 thr:0
  num_consecutive_fail:
  ```

  These messages are caused by an LTE H/M failure caused by an abnormal increment of the fragment lock counter in lookup.

  Workaround: There is currently no known workaround.

- CSCue97620—IXP QM encountered NULL/Invalid buffer handle

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 000246: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/3: 000247: Feb 24 14:52:34:  PLATFORM-1-DP_HM_FAIL  Failed to receive response
from IXP2. Check `sami health-monitoring' configuration and see `show sami
health-monitoring' for more info
SAMI 1/5: 000039: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/8: 000038: Feb 24 14:52:34:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 in 16 retries, system will reboot if it continues to fail receiving
response in another 16 retries (i.e. in the next 256 milliseconds.)</B>
```

These messages are caused when the Cisco SAMI LTE QM encounters NULL/Invalid buffer handle.

Workaround: There is currently no known workaround.

- CSCuh73226—SAMI Qnx kernel crashes

  SAMI gets reloaded with the reason stating "IXP xscale core received". In the LCP core directory, a file by the name ixp#.txt contains the Qnx kernel core dump.

  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)YS04. 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 Cisco LTE SPGW specific caveats in Cisco IOS Release 12.4(24)YS04.

Cisco SAMI Resolved Caveats

The following Cisco SAMI-specific caveat is resolved with Cisco IOS Release 12.4(24)YS04.

- CSCui37952 - QoS Policing not applied on v1 call after Handoff from v2 - v2>v1>v2

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

- CSCue54602 - Qnx io-net process crash

  Show tech has the reload reason to be:

  System returned to ROM by IXP xscale core received...

  There is a core file for the io-net process collected in the LCP core directory.

  io-net process running on xscale (QNX 6.3) had crashed.

Caveats - Cisco IOS Release 12.4(24)YS03

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS03 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 54
- Cisco SAMI Open Caveats, page 56

Cisco LTE SPGW Open Caveats

This section lists the LTE SPGW-specific caveats that are open with Cisco IOS Release 12.4(24)YS03.

- CSCuh72502

  While Ipv6 aggregate list is re-configured under the APN, aggregate list will return freed memory pattern and while removing the APN, Gateway will be crashed.

  This condition occurs when the aggregate list is re-configured in the VRF enabled APN. When an IPv6 aggregate list is added in the VRF enabled APN, it will not take effort as well.

  Workaround: Unconfigure the VRF, then add IPv6 aggregate and configure VRF once again.

- CSCuc00137

  Traceback seen with reading NULL pointer.

  This is seen on active GW during MBR request processing SCU timer expired and reading NULL

  pointer leads the trace-back.

  Workaround: There is currently no known workaround.

- CSCug93865

  Bearer Qos value is 0 in IRI during 3g-4g Handover

  This condition occurs during 3g-4g Handover.

  On 3g-4g Handover, the IRI value should point at the value that is present in new CSR but it points

  at 0.

  Workaround: There is currently no known workaround.

- CSCuh16043

  MD's cannot be provisioned after multiple switchover

  If any failure happens during de-provisioning, then it will lead to stale entry in active and standby.

It could also lead stale in LI server. If we try to do LI provisioning after reload Active, it will fail.

More Information:

1) Provision 2 MD's, one for IRI and another for CC.

2) Reload the active, standby takes over as active.

3) De-Provision the MD's on the current active i.e initial standby.

4) Run SNMP walk command and no output is shown.

5) Now reload the current active i.e initial standby and Initial Active takes over as active again.

6) Now run SNMP walk and no output should be seen and MD's can be provisioned again. But SNMP

walk will give some output because of stale entries in GW. So, GW will not allow further provisioning.

Workaround: There is currently no known workaround.

- CSCuh83201

  The Data volume reported in S-CDR and P-CDR do not match and the S-CDR does not account for the data sent after S1 Hand over.

  This condition occurs during S1 Handover. Modify bearer request is received without ULI change or without ULI IE.

  Workaround: There is currently no known workaround.

- CSCuh84180

  Stale entry is seen in the encap id table.

  This condition occurs while trying to free the last entity from the table that has exhausted.

  Workaround: There is currently no known workaround.

- CSCuh88565

  Irregularity in ULI output in SGW, PGW, TID output and CDR.

  This condition occurs when a User performs handoff from S4-S11-S4. When the user finally lands as S4 user, the SGW mode still retains the old ULI but PGW updates itself with new ULI. The CDR's are also generated incorrectly. This happens only in SGW-PGW mode.

  Workaround: There is currently no known workaround.

- CSCuh22397

  SAMI blade reloaded causing a crashinfo file. The traceback is new type.

  This condition occurred during normal operation.

  Workaround: There is currently no known workaround.

- CSCug94640 - gateway crashed at pgw_send_successful_modify(0x9e63e54)+0x2c8

  The crash is observed when the GW is trying to process the SCU and send Modify Bearer Response.

  This condition occurs when GW is trying to process the SCU and send Modify Bearer Response simultaneously. SCU is received for the PDP and also the delete event is triggered because of an internal event (idle time-out or clear command or path failure etc.).

  In this scenario, if the delete event is processed first then it will go ahead and flush the pending Queue requests and post a delete to the Queue. Now, before processing delete, if there is a context switch and SCU is processed then SCU tries to post a DONE event to Queue. However, since it does not find the corresponding event, accessing invalid memory under PDP structure causes the crash.

Workaround: There is currently no known workaround.

- CSCug60236

  The syslog seen in Spurious memory access and NULL IDB is given below:

  ```
  SAMI 2/6: 010355: Apr  5 12:11:10: %IPV6_FORWARDING-3-NULLIDB: Uninitialized interface
  pointer - ipv6_fib_forw -Process= "IPv6 Input", ipl= 0, pid= 182,  -Traceback= 0x9AC222Cz
  0x819F850z 0x8CF39A8z 0x8CF4134z 0x8CF4188z 0x8F4DD44z 0x836984Cz 0x9AC0F2Cz
  0x9AC27ACz 0x9AC3AD4z 0x9AB91E8z 0x9ABA1F4z 0x9AC20ECz 0x9AC2468z
  0x9ABE6CCz 0x99EEC2Cz
  ```

  This condition occurs after clearing the adj. The GW received by the Uplink traffic have seen this traceback.

  Workaround: There is currently no known workaround.

- CSCug66168

  Spurious memory access is seen while freeing buffer to memory.

  This condition occurs when Downlink data packets are sent, datapath is blocked, buffering enabled and enode-b linktype is IPv4.

  Workaround: There is currently no known workaround.

- CSCuh80527

  Spurious memory access tracebacks is seen on Active SPGW function while doing create-delete-create for V2 PDP.

  Workaround: There is currently no known workaround.

- CSCuh95701

  "Gprs gtp statistics" Uplink and Downlink counters shows wrong values. There is Access-point statistics packets/bytes counter mismatch.

  This condition occurs while sending traffic.

  Workaround: There is currently no known workaround.

- CSCui01296

  Standby device has stale SGSN control paths while exceeding 32k path limit.

  This condition occurs when new sessions are created after path limit is exhausted in the gateway.

  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)YS03.

- CSCtn88798—Sami got stuck at STDBY COLD after reload

  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 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.

- CSCua36249—Xscale shutdown due to QNX crash, reported as UNKNOWN reload reason

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.

- CSCud36564—SAMI reloads - PCI MEs 6 threads reported as hanging in an “initialize” state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  Workaround: There is currently no known workaround.

- CSCue53135—LTE SPGW: Multiple threads in PCI in thread hung state

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 021084: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:2 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021085: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:3 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021086: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:4 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021087: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:5 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021088: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:6 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021089: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:7 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021090: Jan 16 18:16:46: %PLATFORM-0-DP_IXP_PCI_THR_FAIL: IXP:2 PCI
ME, 8 threads hung
```

  These messages are caused by multiple PCI threads in a hung state.

  Workaround: There is currently no known workaround.

- CSCue78169—LTE HM failure due to abnormal incr. of fragment lock counter in lookup

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 022445: Feb  1 20:10:30: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:1
SAMI 1/3: 022446: Feb  1 20:10:31: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:2
SAMI 1/3: 022447: Feb  1 20:10:32: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:3
SAMI 1/3: 022448: Feb  1 20:10:38: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:1
SAMI 1/3: 022449: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:1
SAMI 1/3: 022450: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:2
SAMI 1/3: 022451: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:4 thr:7
num_consecutive_fail:1
SAMI 1/3: 022452: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:2
SAMI 1/3: 022453: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
```

```
num_consecutive_fail:
```

These messages are caused by an LTE H/M failure caused by an abnormal increment of the fragment lock counter in lookup.

Workaround: There is currently no known workaround.

- CSCue97620—IXP QM encountered NULL/Invalid buffer handle

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 000246: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/3: 000247: Feb 24 14:52:34:  PLATFORM-1-DP_HM_FAIL  Failed to receive response
from IXP2. Check `sami health-monitoring' configuration and see `show sami
health-monitoring' for more info
SAMI 1/5: 000039: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/8: 000038: Feb 24 14:52:34:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 in 16 retries, system will reboot if it continues to fail receiving
response in another 16 retries (i.e. in the next 256 milliseconds.)</B>
```

  These messages are caused when an Cisco SAMI LTE QM encounters NULL/Invalid buffer handle.

  Workaround: There is currently no known workaround.

- CSCuh73226

  Xscale Qnx kernel crashes is observed which pointed to me_dump_g_ns as the user process while it was executed.

  Now, there are more kernel crashes reported while executing pdpstats and dumper_cp processes.

  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)YS03. 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

The following SPGW caveat is resolved with Cisco IOS Release 12.4(24)YS03.

- CSCui22612 - DNS IPv6 address not provided for Gn DSB call.

  IPv6 address for a DNS server request is not updated in the "Create PDP Ctxt Response" message for V1 call.

  This condition occurs when v4/v6 DNS request is sent to APN, that is configured with V4/V6 DNS address. Only V4 DNS address is delivered to UE through "Create PDP Ctxt Response". It does not occur for V2 and S4-SGSN.

  More Info: If GW receives DNS[v4/v6] server request for the APN that is configured with V4/V6 DNS address, then it has to deliver DNS address to UE, but it does not happen for V1 call.

Cisco SAMI Resolved Caveats

There are no newly resolved Cisco SAMI caveats with Cisco IOS Release 12.4(24)YS03.

Caveats - Cisco IOS Release 12.4(24)YS02

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS02 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 61

Cisco LTE SPGW Open Caveats

This section lists the LTE SPGW-specific caveats that are open with Cisco IOS Release 12.4(24)YS02.

- CSCuc00137

  Traceback seen with reading NULL pointer.

  This is seen on active GW during MBR request processing SCU timer expired and reading NULL pointer leads the trace-back.

  Workaround: There is currently no known workaround.

- CSCug93865

  Bearer Qos value is 0 in IRI during 3g-4g Handover

  This condition occurs during 3g-4g Handover.

  On 3g-4g Handover, the IRI value should point at the value that is present in new CSR but it points at 0.

  Workaround: There is currently no known workaround.

- CSCuh16043

  MD's cannot be provisioned after multiple switchover

  If any failure happens during de-provisioning, then it will lead to stale entry in active and standby.

  It could also lead stale in LI server. If we try to do LI provisioning after reload Active, it will fail.

  More Information:

1) Provision 2 MD's, one for IRI and another for CC.

2) Reload the active, standby takes over as active.

3) De-Provision the MD's on the current active i.e initial standby.

4) Run SNMP walk command and no output is shown.

5) Now reload the current active i.e initial standby and Initial Active takes over as active again.

6) Now run SNMP walk and no output should be seen and MD's can be provisioned again. But SNMP

walk will give some output because of stale entries in GW. So, GW will not allow further provisioning.

Workaround: There is currently no known workaround.

- CSCuh83201

  The Data volume reported in S-CDR and P-CDR do not match and the S-CDR does not account for the data sent after S1 Hand over.

  This condition occurs during S1 Handover. Modify bearer request is received without ULI change or without ULI IE.

  Workaround: There is currently no known workaround.

- CSCuh84180

  Stale entry is seen in the encap id table.

  This condition occurs while trying to free the last entity from the table that has exhausted.

  Workaround: There is currently no known workaround.

- CSCuh88565

  Irregularity in ULI output in SGW, PGW, TID output and CDR.

  This condition occurs when a User performs handoff from S4-S11-S4. When the user finally lands as S4 user, the SGW mode still retains the old ULI but PGW updates itself with new ULI. The CDR's are also generated incorrectly. This happens only in SGW-PGW mode.

  Workaround: There is currently no known workaround.

- CSCuh22397

  SAMI blade reloaded causing a crashinfo file. The traceback is new type.

  This condition occurred during normal operation.

  Workaround: There is currently no known workaround.

- CSCug94640

  Gateway crashed at pgw_send_successful_modify(0x9e63e54)+0x2c8.

  Workaround: There is currently no known workaround.

- CSCug60236

  The syslog seen in Spurious memory access and NULL IDB is given below:

  SAMI 2/6: 010355: Apr 5 12:11:10: %IPV6_FORWARDING-3-NULLIDB: Uninitialized interface pointer - ipv6_fib_forw -Process= "IPv6 Input", ipl= 0, pid= 182, -Traceback= 0x9AC222Cz 0x819F850z 0x8CF39A8z 0x8CF4134z 0x8CF4188z 0x8F4DD44z 0x836984Cz 0x9AC0F2Cz 0x9AC27ACz 0x9AC3AD4z 0x9AB91E8z 0x9ABA1F4z 0x9AC20ECz 0x9AC2468z 0x9ABE6CCz 0x99EEC2Cz

This condition occurs after clearing the adj. The GW received by the Uplink traffic have seen this traceback.

Workaround: There is currently no known workaround.

- CSCug66168

  Spurious memory access is seen while freeing buffer to memory.

  This condition occurs when Downlink data packets are sent, datapath is blocked, buffering enabled and enode-b linktype is IPv4.

  Workaround: There is currently no known workaround.

- CSCuh80527

  Spurious memory access tracebacks is seen on Active SPGW function while doing create-delete-create for V2 PDP.

  Workaround: There is currently no known workaround.

- CSCuh95701

  "Gprs gtp statistics" Uplink and Downlink counters shows wrong values. There is Access-point statistics packets/bytes counter mismatch.

  This condition occurs while sending traffic.

  Workaround: There is currently no known workaround.

- CSCuh72502

  Aggregate list is added again in the APN and while unconfiguring the APN, Gateway is crashed.

  This condition occurs when the aggregate list is added again. The added list is freed and returns BOD pattern in "show run | s access-point <index>". When the same APN is uncofigured, it tries to delete the already freed list from the apn->apn_v6aggrlist leading it to crash.

  Workaround: There is currently no known workaround.

- CSCui01296

  Standby device has stale SGSN control paths while exceeding 32k path limit.

  This condition occurs when new sessions are created after path limit is exhausted in the gateway.

  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)YS02.

- CSCtn88798—Sami got stuck at STDBY COLD after reload

  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 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.

- CSCua36249—Xscale shutdown due to QNX crash, reported as UNKNOWN reload reason

  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.

- CSCud36564—SAMI reloads - PCI MEs 6 threads reported as hanging in an “initialize” state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  Workaround: There is currently no known workaround.

- CSCue53135—LTE SPGW: Multiple threads in PCI in thread hung state

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 021084: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:2 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021085: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:3 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021086: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:4 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021087: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:5 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021088: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:6 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021089: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:7 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021090: Jan 16 18:16:46: %PLATFORM-0-DP_IXP_PCI_THR_FAIL: IXP:2 PCI
ME, 8 threads hung
```

  These messages are caused by multiple PCI threads in a hung state.

  Workaround: There is currently no known workaround.

- CSCue78169—LTE HM failure due to abnormal incr. of fragment lock counter in lookup

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 022445: Feb  1 20:10:30: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:1
SAMI 1/3: 022446: Feb  1 20:10:31: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:2
SAMI 1/3: 022447: Feb  1 20:10:32: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:3
SAMI 1/3: 022448: Feb  1 20:10:38: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:1
SAMI 1/3: 022449: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:1
SAMI 1/3: 022450: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:2
SAMI 1/3: 022451: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:4 thr:7
num_consecutive_fail:1
SAMI 1/3: 022452: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:2
SAMI 1/3: 022453: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:
```

  These messages are caused by an LTE H/M failure caused by an abnormal increment of the fragment lock counter in lookup.

Workaround: There is currently no known workaround.

- CSCue97620—IXP QM encountered NULL/Invalid buffer handle

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 000246: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
  response from IXP2 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 1/3: 000247: Feb 24 14:52:34:  PLATFORM-1-DP_HM_FAIL  Failed to receive response
  from IXP2. Check `sami health-monitoring' configuration and see `show sami
  health-monitoring' for more info
  SAMI 1/5: 000039: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
  response from IXP2 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 1/8: 000038: Feb 24 14:52:34:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
  response from IXP2 in 16 retries, system will reboot if it continues to fail receiving
  response in another 16 retries (i.e. in the next 256 milliseconds.)</B>
  ```

  These messages are caused when an Cisco SAMI LTE QM encounters NULL/Invalid buffer handle.

  Workaround: There is currently no known workaround.

- CSCuh73226

  Xscale Qnx kernel crashes is observed which pointed to me_dump_g_ns as the user process while it was executed.

  Now, there are more kernel crashes reported while executing pdpstats and dumper_cp processes.

  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)YS02. 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 66

Cisco LTE SPGW Resolved Caveats

The following SPGW caveat is resolved with Cisco IOS Release 12.4(24)YS02.

- CSCug20647 - ServiceChangeCond field in PGW-CDRs not compliant to 32.298 v8.4.0

  Service change condition in service record was updated as bit string instead of octet string.

  Due to this wrong encoding, mediation device is not able to decode this attribute properly and there is out of sync between ASR5k CDRs and SAMI CDRs.

- CSCuh19218 - PGW not deleting session when UBR Response received with cause 64

  Session is not Deleted

  GW does not delete the session when it receives Update Bearer Response with "Context-Not-Found" cause code.

- CSCue40849 - Restart path is wrongly treated as valid even when restart count is 0

  The syslog seen in the field is given below:

```
Dec  4 08:14:37 ALLNTXCZ82SPG03 228011: SAMI 3/4: 225330: Dec  4 10:14:36:
%GTP-4-RESTART_COUNTER_CHANGED: GSN: 166.137.156.205, Sig src addr:
135.211.21.47, TID: 1340015396212957, SGSN 135.211.21.47 Restart counter changed from 0 to
64, reason: Invalid Restart counter change. Ignored
```

The only impact of this condition is that the restart of the remote node is not detected and as a result,

there will be some stale session that will be deleted when the user reconnects.

- CSCue40861 - After P->SP, sessions are not deleted when it receives DSR from old SGW

  After P->SP, sessions are not deleted when it receives DSR from old SGW

  1) Create seperate S and P mode.

  2) Handoff P session to SP mode.

  3) Now send DSR with OI but set (to delete the complete session) to old SGW and it will forward it to PGW.

- CSCug15203 - Stdby traceback - Spurious memory access made at 0x9E96374z reading 0xC

  Traceback is thrown in standby.

  New SGW session comes up for a particular TID and if there is a session existing in the standby for same TID, traceback will be thrown.

- CSCug55296 - Traceback and crash in gprs_show_pdp_imsi_multi_pdn_walker

  Traceback Spurious Access seen in GW.

  Conditions:

  gtp_pdp_mcb_valid

  gprs_show_pdp_imsi_multi_pdn_walker

  rt_walktree_ap

  rt_walktree

  gprs_show_command

  parse_cmd

  show_techsupport_command

  ggsn_show_techsupport_commands.

- CSCug66566 - Clear pdp leads to Stuck PDP when session wait for delete-credit

  Stuck PDP is observed in GW.

  Clear pdp leads to Stuck PDP when sessions wait on delete-credit.

- CSCuh05026 - Crash due to SPGW session lands on SGW session

  SNMP Process restart Detected on AKRNOHCZ21SPG01

  Lot of LTE_GTPV2-4-LTE_GTPV2_REQUEST_FAILED traps were observed before the reload which cannot be seen after reload.

  ```
  May 18 20:15:36 AKRNOHCZ21SPG01 29976502: SAMI 1/7: 5993593: May 18 23:15:36:
  LTE_GTPV2-4-LTE_GTPV2_REQUEST_FAILED  GTPv2 Update Bearer Request failed, GSN: ,
  Remote: 198.228.228.237, IMSI: 13400185334406F4, APN: , Cause: 64: Bearer Non Existent
  ```

  ```
  May 18 20:15:36 AKRNOHCZ21SPG01 5997337: SAMI 1/5: 5997412: May 18 23:15:36:
  LTE_GTPV2-4-LTE_GTPV2_REQUEST_FAILED  GTPv2 Modify Bearer Request failed, GSN: ,
  Remote: 172.26.29.113, IMSI: 0000000000000000, APN: , Cause: 64: Bearer Non Existent.
  ```

- CSCue49395 - Spurious memory access & INVALID_ID

  Spurious memory Traceback and bad id syslog is seen.

  This occurs while deleting the dedicated bearer in active.
- CSCuf22907 - Crash observed @ gsb_remove

  Standby GW crash.

  During V2 to V1 handoff, update event sync to standby. If IPv4 adj freed and GW tries to use/free the freed adj, then GW will crash.
- CSCuh13178 - Different cause code in V1 and v2 response

  Create-context-response returns "Service not supported" cause code instead of "system failure".

  This condition occurs when create pdp context request for V4 user hits V6 APN.
- CSCue97309 - unknown disconnect reason during PDP delete

  Unknown disconnect reason trace back thrown and unknown counter is incremented

  This condition occurs if session deletion happens due to DSR.
- CSCug09965 - CSR parsed successfuly when there is mismatch between PDP type and PAA.

  When there is a mismatch between the PDN type IE (type 99) and PAA IE in CSReq, CSResponse should be rejected with Mandatory IE incorrect. But, currently the GW parses the message successfully and in some cases, the CSRequest is accepted and MS address is allotted to the UE.
- CSCud32883 - DSB | UL pkts are dropped in T-SGW during SP to P Handover.

  UL packets are dropped in SGW process path

  This condition occurs in SGW process path.
- CSCuf85372 - Cause Code For DSB session no DSB Flag set or Indication/common flag IE.

  When a DSB CSR containing no Indication IE or DSB flag not set in the indication IE (For V2) and/or with no common Flag IE or DSB flag not set in Common Flag (For V1 sessions) are directed towards an IPv4 only or IPV6 only APN, then the cause code currently returned is 19 or 130 (New PDP type due to single address bearer only) depending on the session created. However, it should return 18 and 129 (New PDP type due to network preference).

  This happens only in DSB sessions
- CSCug02558 - SGW does not provide correct ip to UE when DSB CSR is sent to v4 APN

  SGW does not provide correct IP to UE when DSB CSR is sent to v4 APN.
- CSCue85876 - QCI check is not happening at Sp call creation

  Create V2 PDP in SP-Mode (Qci value is used as GBR values). However, it should reject if the Qci is GBR values.

  This occurs when creating a session in SP-Mode only. In SGW and PGW Mode, the session is rejected if Qci is GBR value.
- CSCug48562 - SNMP: cGtpTotalDataMsgDropped not shows the mef drop

  cGtpTotalDataMsgDropped does not provide the mef drop counts.

  Create any (v0/v1/v2) version of PDP and send mef traffic. OID cGtpTotalDataMsgDropped will give only the cef drop counts as counter "CEF dropped count" is shown under the **show gprs gtp pdp-context tid <imsi>**
- CSCuh54318 - Stuck PDPs causing IO mem to go low

IO memory goes low on one of the TCOP and it is observed that there are more sessions on this TCOP compared to other TCOPs. Also, the increase in number of PDP's is in SP mode sessions.

The IO memory goes low because lot of PDP's hold IO memory. During a create-over-create scenario, if the PDP is in "Deleting" state, then the create is stored under the MCB. This will be removed when the MCB memory is deleted.

If the PDP is not getting deleted because it is stuck, this pak memory stays forever with the MCB. But for the memory to go low, there should be lot of stuck PDP's. The SP mode PDP gets stuck because of a rare condition between Idle timeout and DSR from MME/SGSN. If there are 10 SP mode stuck PDPs, then all the SP mode PDP's are stuck because of a wrong method in finding the index to get delete credit.

So, if there are creates for all these PDP's, those would stay forever under the MCB causing lot of IO memory to get consumed causing low IO memory.

- CSCuh78792 - SPGW:IMEI value encoding in Radius request

  IMEI attribute will be encoded as hex format in radius messages for v2 sessions.

  When IMEI is received from MME or S4-SGSN, it will be encoded as hex format in accounting messages. For v1 sessions (Gn/Gp SGSN), it will be updated as string format.

- CSCuh19563 - Mem leak observed on Standby after LI switchover test

  Chunk Elements:

  AllocPC Address Size Parent Name

  95BD224 D7A7AEC 12 20CEB57C (MallocLite)

  95BD224 D866564 12 20CEB57C (MallocLite)

  95BD224 D866580 12 20CEB57C (MallocLite)

  This condition occurs when there is bulk sync of LI generic streams.

  More Information: When standby receives the bulk sync requests from Active, it allocates the

  memory but does not get freed after successful set operation.

Cisco SAMI Resolved Caveats

The following Cisco SAMI-specific caveat is resolved with Cisco IOS Release 12.4(24)YS02.

- CSCud37768 - Incorrect reload reason in LCP during sysmgr crash

  Whenever the sysmgr process crashes, LCP's reload reason shows "power-on" instead of sysmgr process crashed. Due to this, reload reason shown in PPCS are also wrong.

  sysmgr_log.<pid>.tar.gz file will be created in dir core: directory of LCP.

- CSCud43085 - IXP:Enable parity check on control store

  SAMI reloads report IXP PCI micro engine thread health monitoring failure. Warning "%PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:<1/2> PCI thread not responding. me:1 thr:<0/1/2/3/4/5> num_consecutive_fail:3 max_retries:3" appear on ppc console.

  When threads in IXP micro engine, which handles configuration messages from ios/ppc is stuck, a parity error in control store (SRAM) which holds the program (micro code), may result in micro engine fetching invalid code or may incorrectly update its program counter.

- CSCue20764 - SRAM Parity Error Not Getting Detected By Xscale SysMgr

  In some of the cases, the SRAM Parity Error is not detected by Xscale SysMgr.

Whenever IXP encounters SRAM/DRAM parity errors it hangs and does not report to LCP. Hereafter, the Xscale will identify the Parity Errors and notify the LCP which in turn displays the Reload reason as SRAM /DRAM parity error.

IXP Xscale core received as a reload reason will not be reported.

Reload Reason is modified in the below format:

- SRAM Parity Errors will be detected by Xscale. This can be identified in Reload reason of PPC and LCP as:

  IXP<Num> SRAM parity error
- DRAM Ecc Errors will be detected by Xscale. This can be identified in Reload Reason of PPC and LCP as:

  IXP<NUM> DRAM ECC error detected
- Qnx Process Crash can be identified in Reload Reason of PPC and LCP as:

  IXP<NUM> process crashed

- CSCuf31175 - Invalid entries in hash chain causing long searches in hash tables

  Following symtoms can be seen due to this issue:

  1. Packet drops at Rx due to No thread

  2. Packet drops due to MCB not found, although MCB could be present

  When the hash element is marked deleted or invalid by PCI engine,(delete mcb), lookup engine still sees that entry been pointed to by the valid element. It leads to long searches in the free chain and finally ending up with element not found.

Caveats - Cisco IOS Release 12.4(24)YS01

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS01 image:

- Open Caveats, page 67
- Resolved Caveats, page 72

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 67
- Cisco SAMI Open Caveats, page 71

Cisco LTE SPGW Open Caveats

This section lists the LTE SPGW-specific caveats that are open with Cisco IOS Release 12.4(24)YS01.

- CSCug20647

Service change condition in service record was updated as bit string instead of octet string.

Due to this wrong encoding mediation, the device was not able to decode this attribute properly and there is out of sync between asr5k cdrs and sami cdrs.

Workaround: There is currently no known workaround.

- CSCuc00137

  Traceback seen with reading NULL pointer.

  This is seen on active GW during MBR request processing SCU timer expired and reading NULL pointer leads the trace-back.

  Workaround: There is currently no known workaround.

- CSCue40849

  Given below is the syslog seen on the field:

  Dec 4 08:14:37 ALLNTXCZ82SPG03 228011: SAMI 3/4: 225330: Dec 4 10:14:36: %GTP-4-RESTART_COUNTER_CHANGED: GSN: 166.137.156.205, Sig src addr: 135.211.21.47, TID: 1340015396212957, SGSN 135.211.21.47 Restart counter changed from 0 to 64, reason: Invalid Restart counter change. Ignored

  There is not much functional impact. The only impact is the restart of the remote node that will not be detected and there will be some stale session which gets deleted when the user reconnects.

  The restart count 0 is being treated as valid even though the node never sent 0 as restart count. So when the node sends the actual restart count, the restart count is not treated as valid and it is ignored.

  Workaround: There is currently no known workaround.

- CSCue40861

  After P->SP, sessions are not deleted when it receives DSR from old SGW

  1) Create seperate S and P mode.

  2) Handoff P session to SP mode.

  3) Now send DSR with OI but set (to delete the complete session) to old SGW and it will forward it to PGW.

  Workaround: There is currently no known workaround.

- CSCug15203

  Traceback is thrown in standby.

  New SGW session comes up for a particular TID and if there is a session existing in the standby for same TID, traceback will be thrown.

  Workaround: There is currently no known workaround.

- CSCug55296

  Traceback Spurious Access seen in GW.

  Conditions:

  gtp_pdp_mcb_valid

  gprs_show_pdp_imsi_multi_pdn_walker

  rt_walktree_ap

  rt_walktree

  gprs_show_command

parse_cmd

show_techsupport_command

ggsn_show_techsupport_commands.

Workaround: There is currently no known workaround.

- CSCug66566

  Stuck PDP is observed in GW.

  Clear pdp leads to Stuck PDP when sessions wait on delete-credit.

  Workaround: "clear gprs gtp pdp-context all local" will clear the stuck PDP.

- CSCuh05026

  SNMP Process restart Detected on AKRNOHCZ21SPG01

  Lot of LTE_GTPV2-4-LTE_GTPV2_REQUEST_FAILED traps were observed before the reload which cannot be seen after reload.

  May 18 20:15:36 AKRNOHCZ21SPG01 29976502: SAMI 1/7: 5993593: May 18 23:15:36: LTE_GTPV2-4-LTE_GTPV2_REQUEST_FAILED GTPv2 Update Bearer Request failed, GSN: , Remote: 198.228.228.237, IMSI: 13400185334406F4, APN: , Cause: 64: Bearer Non Existent

  May 18 20:15:36 AKRNOHCZ21SPG01 5997337: SAMI 1/5: 5997412: May 18 23:15:36: LTE_GTPV2-4-LTE_GTPV2_REQUEST_FAILED GTPv2 Modify Bearer Request failed, GSN: , Remote: 172.26.29.113, IMSI: 0000000000000000, APN: , Cause: 64: Bearer Non Existent.

  Workaround: There is currently no known workaround.

- CSCuh19218

  Session is not Deleted.

  GW does not delete the session when it receives Update Bearer Response with "Context-Not-Found" cause code.

  Workaround: There is currently no known workaround

- CSCue49395

  Spurious memory Traceback and bad id syslog is seen.

  This occurs while deleting the dedicated bearer in active.

  Workaround: There is currently no known workaround

- CSCuf22907

  Standby GW crash.

  During V2 to V1 handoff, update event sync to standby. If IPv4 adj freed and GW tries to use/free the freed adj, then GW will crash.

  Workaround: There is currently no known workaround

- CSCuf47117

  For v2 session, if indication IE is not received from MME, PGW allocates both IPv4 and IPv6 addresses.

  Expected: Since the indication IE is not received. PGW will not have the DSB flag received from MME and should allocate only IPv6 address.

  This behavior is seen only when indication IE is not received from MME.

  Workaround: There is currently no known workaround

- CSCug60236

  The following Spurious memory access and NULL IDB syslog is seen.

  ```
  SAMI 2/6: 010355: Apr  5 12:11:10: %IPV6_FORWARDING-3-NULLIDB: Uninitialized interface
  pointer - ipv6_fib_forw -Process= "IPv6 Input", ipl= 0, pid= 182,  -Traceback= 0x9AC222Cz
  0x819F850z 0x8CF39A8z 0x8CF4134z 0x8CF4188z 0x8F4DD44z 0x836984Cz 0x9AC0F2Cz
  0x9AC27ACz 0x9AC3AD4z 0x9AB91E8z 0x9ABA1F4z 0x9AC20ECz 0x9AC2468z
  0x9ABE6CCz 0x99EEC2Cz
  ```

  After clearing the adj, GW receives the Uplink traffic have seen this traceback.

  Workaround: There is currently no known workaround

- CSCuh13178

  Create-context-response returns "Service not supported" cause code instead of "No Resource available".

  This condition occurs when IP address pool is not configured on APN.

  Workaround: There is currently no known workaround

- CSCug93865

  Bearer Qos value is 0 in IRI during 3g-4g Handover

  This condition occurs during 3g-4g Handover.

  On 3g-4g Handover, the IRI value should point at the value that is present in new CSR but it points at 0.

  Workaround: There is currently no known workaround

- CSCuh16043

  MD's cannot be provisioned after multiple switchover

  If any failure happens during de-provisioning, then it will lead to stale entry in active and standby. It could also lead stale in LI server. If we try to do LI provisioning after reload Active, it will fail.

  More Information:

  1) Provision 2 MD's, one for IRI and another for CC.

  2) Reload the active, standby takes over as active.

  3) De-Provision the MD's on the current active i.e initial standby.

  4) Run snmp walk command and no output is shown.

  5) Now reload the current active i.e initial standby and Initial Active takes over as active again.

  6) Now run snmp walk and no o/p should be seen and MD's can be provisioned again. But snmp walk will give some o/p because of stale entries in GW. So, GW will not allow further provisioning.

  Workaround: There is currently no known workaround

- CSCuh19563

  Mem leak observed on Standby after LI switchover test

  ```
  Chunk Elements:
  AllocPC  Address    Size   Parent   Name
  95BD224  D7A7AEC    12 20CEB57C (MallocLite)
  95BD224  D866564    12 20CEB57C (MallocLite)
  95BD224  D866580    12 20CEB57C (MallocLite)
  ```

This condition occurs when there is bulk sync of LI generic streams.

More Information: When standby receives the bulk sync requests from Active, it allocates the memory but does not get freed after successful set operation..

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)YS01.

- CSCtn88798—Sami got stuck at STDBY COLD after reload

  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.

- CSCua36249—Xscale shutdown due to QNX crash, reported as UNKNOWN reload reason

  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.

- CSCud36564—SAMI reloads - PCI MEs 6 threads reported as hanging in an “initialize” state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  Workaround: There is currently no known workaround.

- CSCue53135—LTE SPGW: Multiple threads in PCI in thread hung state

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 021084: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:2 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021085: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:3 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021086: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:4 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021087: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:5 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021088: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:6 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021089: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:7 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021090: Jan 16 18:16:46: %PLATFORM-0-DP_IXP_PCI_THR_FAIL: IXP:2 PCI
  ME, 8 threads hung
  ```

  These messages are caused by multiple PCI threads in a hung state.

  Workaround: There is currently no known workaround.

- CSCue78169—LTE HM failure due to abnormal incr. of fragment lock counter in lookup

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 022445: Feb  1 20:10:30: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
  me:14 thr:5
  ```

```
num_consecutive_fail:1
SAMI 1/3: 022446: Feb  1 20:10:31: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:2
SAMI 1/3: 022447: Feb  1 20:10:32: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:3
SAMI 1/3: 022448: Feb  1 20:10:38: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:1
SAMI 1/3: 022449: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:1
SAMI 1/3: 022450: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:2
SAMI 1/3: 022451: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:4 thr:7
num_consecutive_fail:1
SAMI 1/3: 022452: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:2
SAMI 1/3: 022453: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:
```

These messages are caused by an LTE H/M failure caused by an abnormal increment of the fragment lock counter in lookup.

Workaround: There is currently no known workaround.

- CSCue97620—IXP QM encountered NULL/Invalid buffer handle

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 000246: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/3: 000247: Feb 24 14:52:34:  PLATFORM-1-DP_HM_FAIL  Failed to receive response
from IXP2. Check `sami health-monitoring' configuration and see `show sami
health-monitoring' for more info
SAMI 1/5: 000039: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/8: 000038: Feb 24 14:52:34:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 in 16 retries, system will reboot if it continues to fail receiving
response in another 16 retries (i.e. in the next 256 milliseconds.)</B>
```

  These messages are caused when an Cisco SAMI LTE QM encounters NULL/Invalid buffer handle.

  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)YS01. Only severity 1 and 2 caveats and select severity 3 caveats are listed.

- Cisco LTE SPGW Resolved Caveats, page 73
- Cisco SAMI Resolved Caveats, page 74

Cisco LTE SPGW Resolved Caveats

The following SPGW caveat is resolved with Cisco IOS Release 12.4(24)YS01.

- 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.

- CSCug25026

  Create pdp response contains two extra junk bytes after 'End user addr' IE.

  When create pdp req is sent with DSB flag to v4 only APN.

- 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.

- CSCuf24393

  The MS address is not returned as part of Create Context Response with the cause "New PDP type due to network preference" for v1 DSB request, directed to an APN that supports IPv4 only. The issue is not seen in v2 DSB sessions.

  This condition occurs while creating DSB sessions.

- CSCuf84186

  Create Context Response does not contain the TEID for v1 DSB request that is directed to v4 APN or v6 APN. The issue is not seen in v2 DSB sessions.

  This condition occurs while creating DSB sessions.

- CSCuf73928

  The IPv4 address is not allocated in standby SPGW when a dual stack bearer is created on SPGW. This condition occurs when SPGW gets a dual stack bearer create request from MME (i.e. dual bearer APN, with Indication IE present and DAF set), active node allocates both IPv4 and IPv6 addresses whereas standby node allocates only IPv6 address.

- 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)YS01.

Caveats - Cisco IOS Release 12.4(24)YS

This section contains the following types of caveats that apply to the Cisco LTE SPGW Release 2.3, Cisco IOS Release 12.4(24)YS image:

- Open Caveats, page 74
- Resolved Caveats, page 78

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 74
- 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)YS.

- CSCuc00137—Spurious memory access @ pgw_sm_is_ixp_update_required

  A traceback is seen upon reading NULL pointer.

  This condition is seen on the active Cisco LTE SPGW MBR processing, Service Control Usage (SCU) timer expires, and reading NULL pointer.

  Workaround: There is currently no known workaround.

- CSCuc11009—Crash @ adj_switch_ipv4_generic_les

  The Cisco LTE SPGW crashes at adj_switch_ipv4_generic_les when processing a downlink data packet.

  This condition occurs when processing a downlink data packet. The crash occurs because of some inappropriate length in the packet and gateway calculations.

  Workaround: There is currently no known workaround.

- CSCud29420—Spurious memory access@0x828D350z reading 0x2EC

  The following spurious memory access and bad id syslog is seen on the Cisco LTE SPGW:

```
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 is seen while a dedicated bearer is being deleted in the standby gateway.

Workaround: There is currently no known workaround.

- CSCue40849—Restart path is incorrectly treated as valid even when the restart is 0

  The following syslog is sometimes seen on the Cisco LTE SPGW:

  ```
  Dec  4 08:14:37 ALLNTXCZ82SPG03 228011: SAMI 3/4: 225330: Dec  4 10:14:36:
  %GTP-4-RESTART_COUNTER_CHANGED: GSN: 166.137.156.205, Sig src addr: 135.211.21.47,
  TID: 1340015396212957, SGSN 135.211.21.47 Restart counter changed from 0 to 64,
  reason: Invalid Restart counter change. Ignored
  ```

  The only impact of this condition is that the restart of the remote node is not detected and as a result, there will be some stale session that will be deleted when the user reconnects.

  Workaround: There is currently no known workaround.

- CSCue40861—After P->SP, sessions are not deleted when it receives DSR from old SGW

  After a P-to-SP handoff, sessions are not deleted when the gateway receives a DSR from the former SGW. This condition occurs with the following scenario:

  a. Separate S and P mode sessions are created.

  b. The P mode session is handed off to SP mode.

  c. The DSR is sent with OI but sent (to delete the complete session) to the former SGW, which forwards the DSR to the PGW.

  Workaround: There is currently no known workaround.

- CSCue49395—Spurious memory access & INVALID_ID

  A spurious memory traceback and bad ID syslog is seen on the Cisco LTE SPGW.

  This condition occurs while deleting a dedicated bearer on the active gateway.

  Workaround: There is currently no known workaround.

- CSCue50118—Spurious access at sgw_send_downlink_data_notif_interface

  Spurious memory is seen in sgw_send_downlink_data_notif_interface.

  This condition, spurious memory access, is made while trying to get GTP_SOCK_GET_REMOTE_ADDR_V4.

  Workaround: There is currently no known workaround.

- CSCue66481—GW crashed when CDRs are cleared in the GW

  Cisco LTE SPGW crashes when CDRs are cleared in the gateway.

  It is suspected that the condition was caused when the clear was due to manual intervention.

- CSCue78216—S-CDR volume usage issue

  S-CDRs with more than 250MB downlink and uplink volume usage are seen.

This condition occurs when the SGW receives a large number of downstream fragmented packets from the Cisco LTE SPGW. The volume trigger is not functioning as designed and the condition leads to the CDR being closed with high volume usage.

Workaround: There is currently no known workaround.

- CSCuf00649—Active crash scenarios

  The Cisco LTE SPGW might crash.

  This crash occurs when the gateway is processing an Service Control Usage (SCU) message from the Cisco CSG2, if the SPGW has an invalid PDP in the mcb structure.

  Workaround: There is currently no known workaround.

- CSCuf00799—Stdby crash with pdp deletion with removing from accting hash tab

  The Cisco LTE SPGW crashes 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 gateway

Cisco SAMI Open Caveats

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

- CSCtn88798—Sami got stuck at STDBY COLD after reload

  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.

- CSCua36249—Xscale shutdown due to QNX crash, reported as UNKNOWN reload reason

  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.

- CSCud36564—SAMI reloads - PCI MEs 6 threads reported as hanging in an “initialize” state

  A H/M failure occurs and the Cisco SAMI reloads because PCI threads are in a hung state.

  Workaround: There is currently no known workaround.

- CSCue53135—LTE SPGW: Multiple threads in PCI in thread hung state

  The following messages might display on the Cisco LTE SPGW console:

  ```
  SAMI 1/3: 021084: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:2 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021085: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:3 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021086: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:4 num_consecutive_fail:3 max_retries:3
  SAMI 1/3: 021087: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
  thread not responding. me:1 thr:5 num_consecutive_fail:3 max_retries:3
  ```

```
SAMI 1/3: 021088: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:6 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021089: Jan 16 18:16:46: %PLATFORM-3-DP_IXP_PCI_THR_WARN: IXP:2 PCI
thread not responding. me:1 thr:7 num_consecutive_fail:3 max_retries:3
SAMI 1/3: 021090: Jan 16 18:16:46: %PLATFORM-0-DP_IXP_PCI_THR_FAIL: IXP:2 PCI
ME, 8 threads hung
```

These messages are caused by multiple PCI threads in a hung state.

Workaround: There is currently no known workaround.

- CSCue78169—LTE HM failure due to abnormal incr. of fragment lock counter in lookup

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 022445: Feb  1 20:10:30: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:1
SAMI 1/3: 022446: Feb  1 20:10:31: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:2
SAMI 1/3: 022447: Feb  1 20:10:32: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:14 thr:5
num_consecutive_fail:3
SAMI 1/3: 022448: Feb  1 20:10:38: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:1
SAMI 1/3: 022449: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:1
SAMI 1/3: 022450: Feb  1 20:10:39: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:2
SAMI 1/3: 022451: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:4 thr:7
num_consecutive_fail:1
SAMI 1/3: 022452: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:9 thr:4
num_consecutive_fail:2
SAMI 1/3: 022453: Feb  1 20:10:40: %PLATFORM-3-DP_IXP_THR_WARN: IXP:2 thread blocked.
me:10 thr:0
num_consecutive_fail:
```

  These messages are caused by an LTE H/M failure caused by an abnormal increment of the fragment lock counter in lookup.

  Workaround: There is currently no known workaround.

- CSCue97620—IXP QM encountered NULL/Invalid buffer handle

  The following messages might display on the Cisco LTE SPGW console:

```
SAMI 1/3: 000246: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/3: 000247: Feb 24 14:52:34:  PLATFORM-1-DP_HM_FAIL  Failed to receive response
from IXP2. Check `sami health-monitoring' configuration and see `show sami
health-monitoring' for more info
SAMI 1/5: 000039: Feb 24 14:52:33:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 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 1/8: 000038: Feb 24 14:52:34:  PLATFORM-2-DP_IXP_HM_WARN  Failed to receive
response from IXP2 in 16 retries, system will reboot if it continues to fail receiving
response in another 16 retries (i.e. in the next 256 milliseconds.)</B>
```

  These messages are caused when an Cisco SAMI LTE QM encounters NULL/Invalid buffer handle.

Workaround: There is currently no known workaround.

Resolved Caveats

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

- Cisco LTE SPGW Resolved Caveats, page 78
- Cisco SAMI Resolved Caveat, page 80

Cisco LTE SPGW Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.4(24)YS

- CSCtx62235—PGW sends CDR data out of order after being flow controlled.

  After the charging gateway removes flow control, 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 previously sending.

- CSCty22796—CLI: single ip aaa server stats not aggregated to proc3

  The CISCO-AAA-SERVER-MIB casStatisticsTable returns zeros for statistics. The **show aaa servers** command output also returns zeros for statistics, however an **execute-on all** command output shows nonzero stats on Traffic and Control Plane Processors (4-8).

  This condition occurs under normal condition.

- CSCuc73657— GW_SR_EVENT_PDP_GTP_UPDATE_MODIFY_BEARER syslog seen during TAU/RAU HO

  A huge number of event logs (GW_SR_EVENT_PDP_GTP_UPDATE_MODIFY_BEARER) are seen on the standby gateway during a TAU-RAU handoff and the handoff fails.

  During 3G-to-4G continuous handoffs, these syslogs are seen and there are failures in the handoff.

- CSCuc84209—Traceback Detected@0x82C5EC0z reading 0xD4

  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 the active SPGW when the **show gprs gtp pdp tid all** command is executed.

- CSCud49673—Spurious memory@0x9EA8DD0z reading 0x6

  The following spurious access is seen on the Cisco LTE SPGW:

```
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
```

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

- CSCud82669—Overlap in 3gpp-Charging-ID in GW dual-reload scenario

  The SPGW generates a unique charging-id for each PDP. There is a chance that the charging-id might be reused (overlapped) during a double reload.

  The following is a scenario of when the condition might occur:

  a. GW-1 is active and GW-2 is standby.

  b. GW-1 reloads.

  c. GW-2 becomes active and starts accepting new PDP create requests.

  d. GW-2 reloads before GW-1 comes up.

  e. When GW-1 comes up, it becomes active again.

  f. GW-1 starts creating PDPs. However, the charging id allocated by GW-1 overlaps with those allocated by GW-2 in step C.

- CSCud91060—Crash @ list_remove_default process

  A crash occurs at “list_remove_default” process.

- CSCue27573—GW crashed due to bad refcnt in a chunk allocated for a AAA related data

  An active SPGW reloads due to memory corruption (“CHUNKBADREFCOUNT”) in the AAA data of a PDP.

  This condition occurs with the very rare scenario where an accounting-start response from Radius is applied to the “wrong” PDP on the SPGW. If this accounting-start has failed, then the SPGW inadvertently deletes a PDP which is unrelated to this accounting transaction.

  The following is an example of the scenario:

  a. The SPGW receives a GTPv1 PDP create request. It sends an accounting-start request to the PCEF and waits for a response.

  b. At this point, the SPGW receives another create request for the same PDP.

  c. The SPGW deletes the existing PDP and attempts to create a new PDP. The SPGW sends a new accounting-start to the PCEF.

  d. At the same time, a failure response arrives for the first accounting-start. The SPGW inadvertently deletes the newly created PDP.

- CSCue56496—Memory leak in standby during MBR without data path

  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.

- CSCue58710— CEF traffic can trigger volume limit for a MEF PDP causing inconsistency

  The SGW S-CDR with service records for User Location ID (ULI) change is counted twice.

This condition occurs when only with a ULI change. The Cisco LTE SPGW reads the PDPs byte counts from the Cisco SAMI IXP and adds a service container in the CDR. If another ULI change occurs, then the SPGW reads counters from the IXP and adds another service record, including the counts that were already added in the first volume container.

The following is an example scenario:

a. A 4G user is present in the SGW and PGW separately.

b. MBReq with new ULI is received by SGW. The SGW reads PDP byte counts from the IXP, adds a new service record to open CDR.

c. Another MBReq with new ULI is received by SGW. The SGW reads the IXP byte counts, adds another service record to open CDR.

d. The CDR is closed and sent to the charging gateway (for any trigger, such as MME change, user delete, etcetera), with second service record having wrong volume usage.

- CSCue70780—Memory leak on gprs_chrg_init_egcdr_cb

  A memory leak in the "EGGSN" and "EGCDR" sub blocks occurs in the standby device.

  This condition can occur with one of the following PGW-mode session creation failures in the standby gateway.

  – Signaling or data path setup failure.

  – Session recreation failure due to some error indication.

  – Insertion in Radix tree failure.

- CSCue73476—After v2->v1->v2 HO ServingNodeType,ULI & RAT not updated in the Standby

  During a SPGW GTPv2-to-GTPv1-to-PGW GTPv2 handoff serving node type, the User Location Information (ULI) and Radio Access Technology (RAT) are not updated properly in standby.

  This condition occurs only when there are multiple handoffs occurring, like GTPv2-to-GTPv1 and then GTPv1-to-GTPv2. After the second handoff completes, the standby CDR values are not synchronized with the active gateway and when the active gateway reloads during this time, the newly-active gateway sends the wrong values in the CDR to the charging gateway.

  Subsequent CDRs have the correct ULI and serving node type, but RAT continues to be sent with an incorrect value.

- CSCue86771—ULI value as Zeros in CDR during v1-pgw/spgw and plmn zero for v1 - spgw

  During a GTPv1-to-GTPv2 (PGW/SPGW) handoff, the User Location Information (ULI) is updated as zeros in the standby gateway CDR.

  This condition occurs only when performing a handoff from GTPv1-to-GTPv2. After the handoff, the version type of the CDR is not set and therefore, it is showing ULI as zeros. The ULI is properly updated but due to version mismatch, it is not updating properly in the CDR that is sent to charging gateway once the standby becomes active.

Cisco SAMI Resolved Caveat

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

- CSCue20323—Uplink Traffic getting dropped at IXP Queue Manager

  Uplink traffic from the UE is unable to reach the Internet because the gateway does not forward the same data.

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

Related Documentation

Except for feature modules, documentation is available as printed manuals or electronic documents. Feature modules are available online on Cisco.com.

Use these release notes with these documents:

- Release-Specific Documents, page 81
- Platform-Specific Documents, page 81
- Cisco IOS Software Documentation Set, page 82

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(24)YS, see the *Cisco LTE SPGW Configuration Guide*.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), 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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only.