Release Change Reference, StarOS Release 21.27

First Published: 2022-04-14

Last Modified: 2022-06-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

About this Guide

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This RCR is applicable to the ASR5500, VPC-DI, and VPC-SI platforms. This RCR describes new and modified feature and behavior change information for the applicable StarOS release(s).

• Conventions Used, on page iii

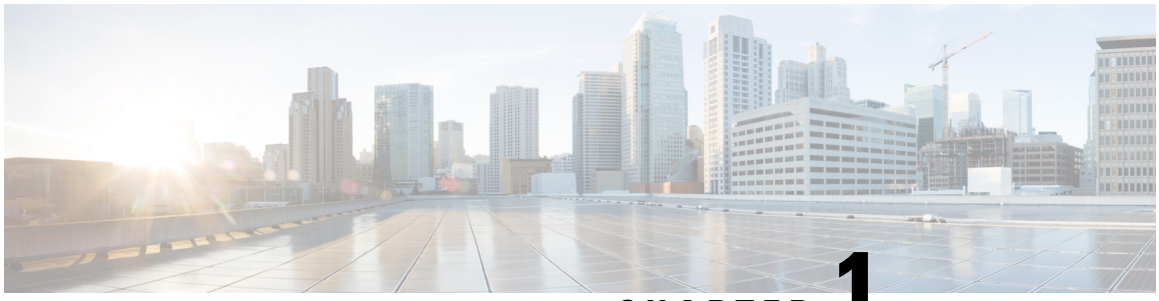
Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`

Typeface Conventions	Description
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**



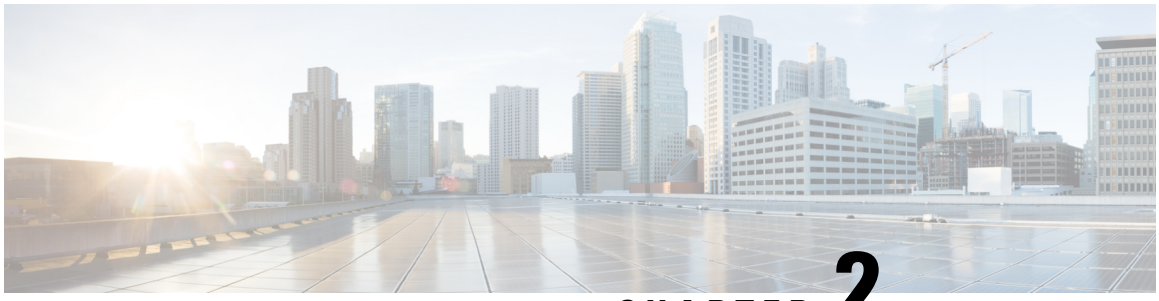
CHAPTER 1

Release 21.27 Features and Changes Quick Reference

Release 21.27 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Addition of Server Unreachable Field in CDR	• GGSN • P-GW • SAEGW	21.27
Capability to Record and Produce Call Transactions, on page 39	• ePDG • P-GW • SaMOG	21.27
Cloud Initialization Support for Elastic Services Controller, on page 61	StarOS	21.27
Customizing Access-Link IP Fragmentation	• GGSN • P-GW • SAEGW	21.27
Configuring SRP Checkpoint, on page 67	StarOS	21.27.m0
Deprecated CLI for MME Initiated PDN Disconnection, on page 69	MME	21.27.2
ePDG Support on VPC-DI, on page 75	ePDG	21.27

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
ePDG Interworking with SMF+P-GW-IWK Support, on page 77	ePDG	21.27
Enable mme clear-route-multipath-zero in CLI, on page 71	MME	21.27
Enforcing Detach on Last PDN Deactivation, on page 73	MME	21.27
IKEv2 Authentication Failure Counters, on page 103	ePDG	21.27
LTE-M RAT Indication Support	MME	21.27
No IMSI or MSISDN Included in LRR for VoLTE EM Call from User of Foreign Network, on page 111	MME	21.27
P2P Signing Process in StarOS, on page 113	StarOS	21.27
SaMOG Support on VPC-DI, on page 115	SaMOG	21.27
Support for 187 and 188 Information Element Types on S2b Interface, on page 117	ePDG	21.27.m0
Support for 187 and 188 Information Element Types on S5 and S8 Interfaces, on page 121	MME	21.27.m0
TCP Robustness Compliance with RFC 5961 , on page 125	P-GW	21.27
Timestamp Accuracy Improvement, on page 129	P-GW	21.27
VLR Management	MME	21.27



CHAPTER 2

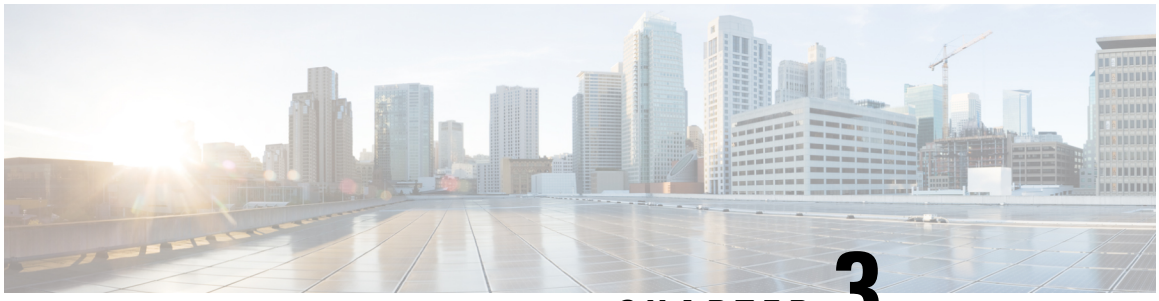
Feature Defaults Quick Reference

Feature Defaults

The following table indicates what features are enabled or disabled by default.

Feature	Default
Addition of Server Unreachable Field in CDR	Disabled - Configuration Required
Capability to Record and Produce Call Transactions	Disabled - Configuration Required
Cloud Initialization Support for Elastic Services Controller	Enabled - Always-on
Configuring Access-Link Fastpath to Enforce APN MTU for IPv4 Traffic	Enabled - Always-on
Configuring SRP Checkpoint	Disabled - Configuration Required
Deprecated CLI for MME Initiated PDN Disconnection	Disabled - Configuration Required
ePDG Support on VPC-D	Disabled - Configuration Required
ePDG Interworking with SMF+P-GW-IWK Support	Disabled - License Required
Enable mme clear-route-multipath-zero in CLI	Disabled - Configuration Required
Enforcing Detach on Last PDN Deactivation	Disabled - Configuration Required
IKEv2 Authentication Failure Counters	Disabled - Configuration Required
LTE-M RAT Indication Support	Disabled - Configuration Required
No IMSI or MSISDN Included in LRR for VoLTE EM Call from User of Foreign Network	Disabled - Configuration Required
SaMOG Support on VPC-DI	Disabled - Configuration Required
Support for 187 and 188 Information Element Types on S2b Interface	Disabled - Configuration Required

Feature	Default
Support for 187 and 188 Information Element Types on S5 and S8 Interfaces	Disabled - Configuration Required
TCP RESET Support	Disabled - Configuration Required
Timestamp Accuracy Improvement	Disabled - Configuration Required
VLR Round-Robin Load Balancing	Disabled - Configuration Required



CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.27 software release.

Important For more information regarding bulk statistics identified in this section, see the latest version of the *BulkstatStatistics_document.xls* spreadsheet supplied with the release.

Bulk statistics changes for 21.27 include:

- New Bulk Statistics, on page 5
- Modified Bulk Statistics, on page 32
- Deprecated Bulk Statistics, on page 32

New Bulk Statistics

ePDG Schema

The following bulkstatistics are added in the ePDG schema as part of the IKEv2 Authentication Failure Counters feature.

Bulk Statistics Variables	Description
ikev2-auth-failnodea	The total number of non DEA messages.
ikev2-auth-failinvresoravp	The total number of invalid result code or AVP in the DEA message.
ikev2-auth-failmissingavp	The total number of missing AVPs in the DEA message.
ikev2-auth-failinvnaiformat	The total number of invalid NAI formats.
ikev2-auth-failinvapn	The total number of invalid APNs.
ikev2-auth-failapnvalfailed	The total number of failed APN validations.

Bulk Statistics Variables	Description
ikev2-auth-failkeymismatch	The total number of key mismatches in the authentication vectors.
ikev2-auth-failmiscauth	The total number of miscellaneous authentication failures.

SaMOG Schema

The following bulkstatistics are added in the SaMOG schema as a part of the Capability to Record and Produce Call Transactions feature.

Bulk Statistics Variables	Description
sess-samog-total-number-event-records	The total number of SaMOG session event records.
sess-samog-total-s2a-event-records	The total number of SaMOG S2a event records.
sess-samog-total-csr-event-records	The total number of SaMOG CSR event records.
sess-samog-total-cbr-event-records	The total number of SaMOG CBR event records.
sess-samog-total-dsr-event-records	The total number of SaMOG DSR event records.
sess-samog-total-dbr-event-records	The total number of SaMOG DBR event records.
sess-samog-total-ubr-event-records	The total number of SaMOG UBR event records.
sess-samog-total-ipv6-ra-event-records	The total number of SaMOG IPv6 RA event records.
sess-samog-total-ra-prefix-event-records	The total number of SaMOG RA prefix event records.
sess-samog-total-dhcpv4-event-records	The total number of SaMOG DHCPv4 event records.
sess-samog-total-dhcpv4-disc-offer-event-records	The total number of SaMOG DHCPv4 discovery offer event records.
sess-samog-total-dhcpv4-req-ack-event-records	The total number of SaMOG DHCPv4 request acknowledgement event records.
sess-samog-total-dhcpv4-rel-ack-event-records	The total number of SaMOG DHCPv4 release acknowledgement event records.
sess-samog-total-rad-auth-event-records	The total number of SaMOG Radius Authentication event records.
sess-samog-total-rad-auth-acc-req-chal-event-records	The total number of SaMOG Radius Authentication access request challenge event records.
sess-samog-total-rad-auth-acc-req-acpt-event-records	The total number of SaMOG Radius Authentication access request accepted event records.
sess-samog-total-rad-auth-disc-req-event-records	The total of number SaMOG Radius Authentication disconnect request event records.

Bulk Statistics Variables	Description
sess-samog-total-rad-acct-event-records	The total number of SaMOG Radius Accounting event records.
sess-samog-total-rad-acct-wlc-event-records	The total number of SaMOG Radius Accounting event records from Wireless LAN Controller.
aaa-samog-total-rad-acct-aaa-event-records	The total number of SaMOG Radius Accounting event records to AAA.
aaa-samog-total-sta-event-records	The total number of SaMOG STa event records.
aaa-samog-total-sta-aar-event-records	The total number of SaMOG STa AAR event records.
aaa-samog-total-sta-der-event-records	The total number of SaMOG STa DER event records.
aaa-samog-total-sta-asr-event-records	The total number of SaMOG STa ASR event records.
aaa-samog-total-sta-rar-event-records	The total number of SaMOG STa RAR event records.
aaa-samog-total-sta-str-event-records	The total number of SaMOG STa STR event records.

MME Schema

The following bulkstatistics are added in the MME schema as part of the LTE M-RAT Indication Support feature.

Variables	Description
LTE-M Attached Calls	The current total number of attached low power Subscribers which are operating in Category M.

Table 1: Bulk Statistic Variables in the P-GW Service Schema

Variables	Description	Data Type
subdatastat-totuppktfwd-64b	Subscriber Data Statistics - Total Uplink packets forwarded **Type:** Counter	Int64
subdatastat-uppktfwd-qci1-64b	Subscriber Data Statistics -Uplink packets forwarded - QCI 1 **Type:** Counter	Int64
subdatastat-uppktfwd-qci2-64b	Subscriber Data Statistics -Uplink packets forwarded - QCI 2 **Type:** Counter	Int64
subdatastat-uppktfwd-qci3-64b	Subscriber Data Statistics -Uplink packets forwarded - QCI 3 **Type:** Counter	Int64

Variables	Description	Data Type
subdatastat-uppktfwd-qci4-64b	Subscriber Data Statistics -Uplink packets forwarded - QCI 4 **Type:** Counter	Int64
subdatastat-uppktfwd-qci5-64b	Subscriber Data Statistics -Uplink packets forwarded - QCI 5 **Type:** Counter	Int64
subdatastat-uppktfwd-qci6-64b	Subscriber Data Statistics -Uplink packets forwarded - QCI 6 **Type:** Counter	Int64
subdatastat-uppktfwd-qci7-64b	Subscriber Data Statistics -Uplink packets forwarded - QCI 7 **Type:** Counter	Int64
subdatastat-uppktfwd-qci8-64b	Subscriber Data Statistics -Uplink packets forwarded - QCI 8 **Type:** Counter	Int64
subdatastat-uppktfwd-qci9-64b	Subscriber Data Statistics -Uplink packets forwarded - QCI 9 **Type:** Counter	Int64
subdatastat-uppktfwd-stdqcinongbr-64b	Subscriber Data Statistics - Uplink packets forwarded - Standard QCI (Non-GBR) **Type:** Counter	Int64
subdatastat-uppktfwd-stdqcigbr-64	Subscriber Data Statistics - Uplink packets forwarded - Standard QCI (GBR) **Type:** Counter	Int64
subdatastat-uppktfwd-qcinongbr-64b	Subscriber Data Statistics - Uplink packets forwarded - Non-Standard QCI (Non-GBR) **Type:** Counter	Int64
subdatastat-uppktfwd-qcigbr-64b	Subscriber Data Statistics - Uplink packets forwarded - Non-Standard QCI (GBR) **Type:** Counter	Int64
subdatastat-uppktfwd-totgbr-64b	Subscriber Data Statistics - Uplink packets forwarded - Total GBR **Type:** Counter	Int64

Variables	Description	Data Type
subdatastat-uppktfwd-totnongbr-64b	Subscriber Data Statistics - Uplink packets forwarded - Total Non-GBR **Type:** Counter	Int64
subdatastat-totulpktfwd-s5-64b	Interface Data Statistics - Uplink packets forwarded **Type:** Counter	Int64
subdatastat-totulpktfwd-s8-64b	Interface Data Statistics - Uplink packets forwarded **Type:** Counter	Int64
subdatastat-totulpktfwd-s2a-64b	Interface Data Statistics - Uplink packets forwarded **Type:** Counter	Int64
subdatastat-totulpktfwd-s2b-64b	Interface Data Statistics - Uplink packets forwarded **Type:** Counter	Int64
subdatastat-uppktfwd-qci65-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 65 **Type:** Counter	Int64
subdatastat-uppktfwd-qci66-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 66 **Type:** Counter	Int64
subdatastat-uppktfwd-qci69-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 69 **Type:** Counter	Int64
subdatastat-uppktfwd-qci70-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 70 **Type:** Counter	Int64
subdatastat-uppktfwd-qci80-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 80 **Type:** Counter	Int64

Variables	Description	Data Type
subdatastat-uppktfwd-qci82-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 82 **Type:** Counter	Int64
subdatastat-uppktfwd-qci83-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 83 **Type:** Counter	Int64
subdatastat-totdownpktfwd-64b	Subscriber Data Statistics - Total Downlink packets forwarded **Type:** Counter	Int64
subdatastat-downpktfwd-qci1-64b	Subscriber Data Statistics - Downlink packets forwarded - QCI 1 **Type:** Counter	Int64
subdatastat-downpktfwd-qci2-64b	Subscriber Data Statistics - Downlink packets forwarded - QCI 2 **Type:** Counter	Int64
subdatastat-downpktfwd-qci3-64b	Subscriber Data Statistics - Downlink packets forwarded - QCI 3 **Type:** Counter	Int64
subdatastat-downpktfwd-qci4-64b	Subscriber Data Statistics - Downlink packets forwarded - QCI 4 **Type:** Counter	Int64
subdatastat-downpktfwd-qci5-64b	Subscriber Data Statistics - Downlink packets forwarded - QCI 5 **Type:** Counter	Int64
subdatastat-downpktfwd-qci6-64b	Subscriber Data Statistics - Downlink packets forwarded - QCI 6 **Type:** Counter	Int64
subdatastat-downpktfwd-qci7-64b	Subscriber Data Statistics - Downlink packets forwarded - QCI 7 **Type:** Counter	Int64
subdatastat-downpktfwd-qci8-64b	Subscriber Data Statistics - Downlink packets forwarded - QCI 8 **Type:** Counter	Int64

Variables	Description	Data Type
subdatastat-downpktfwd-qci9-64b	Subscriber Data Statistics - Downlink packets forwarded - QCI 9 **Type:** Counter	Int64
subdatastat-downpktfwd-stdqcinongbr-64b	Subscriber Data Statistics - Downlink packets forwarded - Standard QCI (Non-GBR) **Type:** Counter	Int64
subdatastat-downpktfwd-stdqcigbr-64b	Subscriber Data Statistics - Downlink packets forwarded - Standard QCI (GBR) **Type:** Counter	Int64
subdatastat-downpktfwd-qcinongbr-64b	Subscriber Data Statistics - Downlink packets forwarded - Non-Standard QCI (Non-GBR) **Type:** Counter	Int64
subdatastat-downpktfwd-qcigbr-64b	Subscriber Data Statistics - Downlink packets forwarded - Non-Standard QCI (GBR) **Type:** Counter	Int64
subdatastat-downpktfwd-totgbr-64b	Subscriber Data Statistics - Downlink packets forwarded - Total GBR **Type:** Counter	Int64
subdatastat-downpktfwd-totnongbr-64b	Subscriber Data Statistics - Downlink packets forwarded - Total Non-GBR **Type:** Counter	Int64
subdatastat-totdlpktfwd-s5-64b	Interface Data Statistics -Downlink packets forwarded **Type:** Counter	Int64
subdatastat-totdlpktfwd-s8-64b	Interface Data Statistics -Downlink packets forwarded **Type:** Counter	Int64
subdatastat-totdlpktfwd-s2a-64b	Interface Data Statistics -Downlink packets forwarded **Type:** Counter	Int64
subdatastat-totdlpktfwd-s2b-64b	Interface Data Statistics -Downlink packets forwarded **Type:** Counter	Int64

Variables	Description	Data Type
subdatastat-downpktfwd-qci65-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 65 **Type:** Counter	Int64
subdatastat-downpktfwd-qci66-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 66 **Type:** Counter	Int64
subdatastat-downpktfwd-qci69-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 69 **Type:** Counter	Int64
subdatastat-downpktfwd-qci70-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 70 **Type:** Counter	Int64
subdatastat-downpktfwd-qci80-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 80 **Type:** Counter	Int64
subdatastat-downpktfwd-qci82-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 82 **Type:** Counter	Int64
subdatastat-downpktfwd-qci83-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 83 **Type:** Counter	Int64
Important For information on statistics that are common to all schema see the *Statistics and Counters Overview* chapter.		

The following bulk statistics are added to the SAEGW schema:

Note In 21.27 and later releases, the following bulkstats counters are supported in both INT32 and INT64 data types.

Table 2: Bulk Statistic Variables in the SAEGW Service Schema

Variables	Description	Data Type
pgw-subdatastat-totulpktfwd-64b	P-GW Subscriber Data Statistics: Total Uplink packets forwarded **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci1-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - QCI 1 **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci2-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - QCI 2 **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci3-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - QCI 3 **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci4-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - QCI 4 **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci5-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - QCI 5 **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci6-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - QCI 6 **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci7-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - QCI 7 **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci8-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - QCI 8 **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci9-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - QCI 9 **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci65-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 65 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64

Variables	Description	Data Type
pgw-subdatastat-ulpktfwd-qci66-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 66 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci69-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 69 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci70-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 70 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-stdqcinongbr-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - Standard QCI (Non-GBR) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-stdqcigbr-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - Standard QCI (GBR) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qcinongbr-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - Non-Standard QCI (Non-GBR) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qcigbr-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - Non-Standard QCI (GBR) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-totgbr-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - Total GBR **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-totnongbr-64b	P-GW Subscriber Data Statistics: Uplink packets forwarded - Total Non-GBR **Type:** Counter	Int64
pgw-subdatastat-totdlpktfwd-64b	P-GW Subscriber Data Statistics: Total Downlink packets forwarded **Type:** Counter	Int64

Variables	Description	Data Type
pgw-subdatastat-dlpktfwd-qci1-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - QCI 1 **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci2-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - QCI 2 **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci3-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - QCI 3 **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci4-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - QCI 4 **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci5-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - QCI 5 **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci6-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - QCI 6 **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci7-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - QCI 7 **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci8-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - QCI 8 **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci9-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - QCI 9 **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci65-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 65 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64

Variables	Description	Data Type
pgw-subdatastat-dlpktfwd-qci66-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 66 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci69-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 69 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci70-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 70 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-stdqcinongbr-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - Standard QCI (Non-GBR) **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-stdqcigbr-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - Standard QCI (GBR) **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qcinongbr-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - Non-Standard QCI (Non-GBR) **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qcigbr-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - Non-Standard QCI (GBR) **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-totgbr-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - Total GBR **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-totnongbr-64b	P-GW Subscriber Data Statistics: Downlink packets forwarded - Total Non-GBR **Type:** Counter	Int64

Variables	Description	Data Type
pgw-subdatastat-totdlpktfwd-s5-64b	Interface Data Statistics -Downlink packets forwarded **Type:** Counter	Int64
pgw-subdatastat-totulpktfwd-s5-64b	**Description:** Subscriber Data Statistics - Total Uplink packets forwarded by S5 P-GW in SAEGW setup. **Triggers:** This counter is updated when uplink packet is forwarded by S5 P-GW in SAEGW setup. **Availability:** Per SAEGW Service **Standard or Proprietary**: Proprietary **Type:** Counter	Int64
pgw-subdatastat-totulpktfwd-s8-64b	**Description:** Subscriber Data Statistics - Total Uplink packets forwarded by S8 P-GW in SAEGW setup. **Triggers:** This counter is updated when uplink packet is forwarded by S8 P-GW in SAEGW setup. **Availability:** Per SAEGW Service **Standard or Proprietary**: Proprietary **Type:** Counter	Int64
pgw-subdatastat-totdlpktfwd-s8-64b	**Description:** Subscriber Data Statistics - Total Uplink bytes forwarded by S8 P-GW in SAEGW setup. **Triggers:** This counter is updated when uplink packet is forwarded by S8 P-GW in SAEGW setup. **Availability:** Per SAEGW Service **Standard or Proprietary**: Proprietary **Type:** Counter	Int64

Variables	Description	Data Type
pgw-subdatastat-totulpktfwd-s2a-64b	**Description:** Subscriber Data Statistics - Total Uplink packets forwarded by S2a P-GW in SAEGW setup. **Triggers:** This counter is updated when uplink packet is forwarded by S2a P-GW in SAEGW setup. **Availability:** Per SAEGW Service **Standard or Proprietary**: Proprietary **Type:** Counter	Int64
pgw-subdatastat-totdlpktfwd-s2a-64b	**Description:** Subscriber Data Statistics - Total Uplink bytes forwarded by S2a P-GW in SAEGW setup. **Triggers:** This counter is updated when uplink packet is forwarded by S2a P-GW in SAEGW setup. **Availability:** Per SAEGW Service **Standard or Proprietary**: Proprietary **Type:** Counter	Int64
pgw-subdatastat-totulpktfwd-s2b-64b	**Description:** Subscriber Data Statistics - Total Uplink packets forwarded by S2b P-GW in SAEGW setup. **Triggers:** This counter is updated when uplink packet is forwarded by S2b P-GW in SAEGW setup. **Availability:** Per SAEGW Service **Standard or Proprietary**: Proprietary **Type:** Counter	Int64
pgw-subdatastat-totdlpktfwd-s2b-64b	**Description:** Subscriber Data Statistics - Total Uplink bytes forwarded by S2b P-GW in SAEGW setup. **Triggers:** This counter is updated when uplink packet is forwarded by S2b P-GW in SAEGW setup. **Availability:** Per SAEGW Service **Standard or Proprietary**: Proprietary **Type:** Counter	Int64

Variables	Description	Data Type
pgw-subdatastat-dlpktfwd-qci80-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 80 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci82-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 82 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-dlpktfwd-qci83-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 83 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci80-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 80 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci82-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 82 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
pgw-subdatastat-ulpktfwd-qci83-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 83 on a P-GW (as part of the SAEGW) **Type:** Counter	Int64
collapsed-subdatastat-ulpktfwd-qci1-64b	**Description**: Collapsed Subscriber Data Statistics: Uplink packets forwarded - QCI 1 **Availability**: Per SAEGW service **Trigger**: Increments by 1 at sessmgr (P-GW) for a collapsed call for Quality Class Identifier 1 when the UL data packet is forwarded to Gi by P-GW.The UL packets sent by S-GW (of SAEGW) but dropped at P-GW, are not counted. **Type**: Counter	Int64

Variables	Description	Data Type
collapsed-subdatastat-ulpktfwd-qci2-64b	**Description**: Collapsed Subscriber Data Statistics: Uplink packets forwarded - QCI 2 **Availability**: Per SAEGW service **Trigger**: Increments by 1 at sessmgr (P-GW) for a collapsed call for Quality Class Identifier 2 when the UL data packet is forwarded to Gi by P-GW.The UL packets sent by S-GW (of SAEGW) but dropped at P-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci3-64b	**Description**: Collapsed Subscriber Data Statistics: Uplink packets forwarded - QCI 3 **Availability**: Per SAEGW service **Trigger**: Increments by 1 at sessmgr (P-GW) for a collapsed call for Quality Class Identifier 3 when the UL data packet is forwarded to Gi by P-GW.The UL packets sent by S-GW (of SAEGW) but dropped at P-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci4-64b	**Description**: Collapsed Subscriber Data Statistics: Uplink packets forwarded - QCI 4 **Availability**: Per SAEGW service **Trigger**: Increments by 1 at sessmgr (P-GW) for a collapsed call for Quality Class Identifier 4 when the UL data packet is forwarded to Gi by P-GW.The UL packets sent by S-GW (of SAEGW) but dropped at P-GW, are not counted. **Type**: Counter	Int64

Variables	Description	Data Type
collapsed-subdatastat-ulpktfwd-qci5-64b	**Description**: Collapsed Subscriber Data Statistics: Uplink packets forwarded - QCI 5 **Availability**: Per SAEGW service **Trigger**: Increments by 1 at sessmgr (P-GW) for a collapsed call for Quality Class Identifier 5 when the UL data packet is forwarded to Gi by P-GW.The UL packets sent by S-GW (of SAEGW) but dropped at P-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci6-64b	**Description**: Collapsed Subscriber Data Statistics: Uplink packets forwarded - QCI 6 **Availability**: Per SAEGW service **Trigger**: Increments by 1 at sessmgr (P-GW) for a collapsed call for Quality Class Identifier 6 when the UL data packet is forwarded to Gi by P-GW.The UL packets sent by S-GW (of SAEGW) but dropped at P-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci7-64b	**Description**: Collapsed Subscriber Data Statistics: Uplink packets forwarded - QCI 7 **Availability**: Per SAEGW service **Trigger**: Increments by 1 at sessmgr (P-GW) for a collapsed call for Quality Class Identifier 7 when the UL data packet is forwarded to Gi by P-GW.The UL packets sent by S-GW (of SAEGW) but dropped at P-GW, are not counted. **Type**: Counter	Int64

Variables	Description	Data Type
collapsed-subdatastat-ulpktfwd-qci8-64b	**Description**: Collapsed Subscriber Data Statistics: Uplink packets forwarded - QCI 8 **Availability**: Per SAEGW service **Trigger**: Increments by 1 at sessmgr (P-GW) for a collapsed call for Quality Class Identifier 8 when the UL data packet is forwarded to Gi by P-GW.The UL packets sent by S-GW (of SAEGW) but dropped at P-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci9-64b	**Description**: Collapsed Subscriber Data Statistics: Uplink packets forwarded - QCI 9 **Availability**: Per SAEGW service **Trigger**: Increments by 1 at sessmgr (P-GW) for a collapsed call for Quality Class Identifier 9 when the UL data packet is forwarded to Gi by P-GW.The UL packets sent by S-GW (of SAEGW) but dropped at P-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci65-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 65 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci66-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 66 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci69-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 69 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci70-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 70 on a SAEGW **Type**: Counter	Int64

Variables	Description	Data Type
collapsed-subdatastat-ulpktfwd-qci80-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 80 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci82-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 82 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-ulpktfwd-qci83-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 83 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci1-64b	**Description**: Collapsed Data Statistics: Downlink Statistics - QCI 1 Total-Packets **Availability**: Per SAEGW service **Trigger**: Increments at sessmgr (P-GW) for a collapsed call per Quality of Class Identifier when the DL data packet is forwarded to ENB.The DL packets sent by P-GW (of SAEGW) but dropped at S-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci2-64b	**Description**: Collapsed Data Statistics: Downlink Statistics - QCI 2 Total-Packets **Availability**: Per SAEGW service **Trigger**: Increments at sessmgr (P-GW) for a collapsed call per Quality of Class Identifier 2 when the DL data packet is forwarded to ENB.The DL packets sent by P-GW (of SAEGW) but dropped at S-GW, are not counted. **Type**: Counter	Int64

Variables	Description	Data Type
collapsed-subdatastat-dlpktfwd-qci3-64b	**Description**: Collapsed Data Statistics: Downlink Statistics - QCI 3 Total-Packets **Availability**: Per SAEGW service **Trigger**: Increments at sessmgr (P-GW) for a collapsed call per Quality of Class Identifier 3 when the DL data packet is forwarded to ENB.The DL packets sent by P-GW (of SAEGW) but dropped at S-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci4-64b	**Description**: Collapsed Data Statistics: Downlink Statistics - QCI 4 Total-Packets **Availability**: Per SAEGW service **Trigger**: Increments at sessmgr (P-GW) for a collapsed call per Quality of Class Identifier 4 when the DL data packet is forwarded to ENB.The DL packets sent by P-GW (of SAEGW) but dropped at S-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci5-64b	**Description**: Collapsed Data Statistics: Downlink Statistics - QCI 5 Total-Packets **Availability**: Per SAEGW service **Trigger**: Increments at sessmgr (P-GW) for a collapsed call per Quality of Class Identifier 5 when the DL data packet is forwarded to ENB.The DL packets sent by P-GW (of SAEGW) but dropped at S-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci6-64b	**Description**: Collapsed Data Statistics: Downlink Statistics - QCI 6 Total-Packets **Availability**: Per SAEGW service **Trigger**: Increments at sessmgr (P-GW) for a collapsed call per Quality of Class Identifier 6 when the DL data packet is forwarded to ENB.The DL packets sent by P-GW (of SAEGW) but dropped at S-GW, are not counted. **Type**: Counter	Int64

Variables	Description	Data Type
collapsed-subdatastat-dlpktfwd-qci7-64b	**Description**: Collapsed Data Statistics: Downlink Statistics - QCI 7 Total-Packets **Availability**: Per SAEGW service **Trigger**: Increments at sessmgr (P-GW) for a collapsed call per Quality of Class Identifier 7 when the DL data packet is forwarded to ENB.The DL packets sent by P-GW (of SAEGW) but dropped at S-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci8-64b	**Description**: Collapsed Data Statistics: Downlink Statistics - QCI 8 Total-Packets **Availability**: Per SAEGW service **Trigger**: Increments at sessmgr (P-GW) for a collapsed call per Quality of Class Identifier 8 when the DL data packet is forwarded to ENB.The DL packets sent by P-GW (of SAEGW) but dropped at S-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci9-64b	**Description**: Collapsed Data Statistics: Downlink Statistics - QCI 9 Total-Packets **Availability**: Per SAEGW service **Trigger**: Increments at sessmgr (P-GW) for a collapsed call per Quality of Class Identifier 9 when the DL data packet is forwarded to ENB.The DL packets sent by P-GW (of SAEGW) but dropped at S-GW, are not counted. **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci65-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 65 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci66-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 66 on a SAEGW **Type**: Counter	Int64

Variables	Description	Data Type
collapsed-subdatastat-dlpktfwd-qci69-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 69 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci70-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 70 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci80-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 80 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci82-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 82 on a SAEGW **Type**: Counter	Int64
collapsed-subdatastat-dlpktfwd-qci83-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 83 on a SAEGW **Type**: Counter	Int64
saegw-ggsn-subdatastat-totulpktfwd-64b	**Description:** GGSN-anchored Subscriber Data Stats - Total Uplink packets forwarded **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-stdqcinongbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - Std QCI (Non-GBR) **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-stdqcigbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - Std QCI (GBR) **Availability:** Per SAEGW service **Type:** Counter	Int64

Variables	Description	Data Type
saegw-ggsn-subdatastat-ulpktfwd-qcinongbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - Non-Std QCI (Non-GBR) **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qcigbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - Non-Std QCI (GBR) **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-totgbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - Total GBR **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-totnongbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - Total Non-GBR **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci80-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 80 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci82-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 82 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci83-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 83 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64
saegw-ggsn-subdatastat-totdlpktfwd-64b	**Description:** GGSN-anchored Subscriber Data Stats - Total Downlink packets forwarded **Availability:** Per SAEGW service **Type:** Counter	Int64

Variables	Description	Data Type
saegw-ggsn-subdatastat-dlpktfwd-qci1-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - QCI 1 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci2-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - QCI 2 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci3-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - QCI 3 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci4-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - QCI 4 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci5-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - QCI 5 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci6-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - QCI 6 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci7-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - QCI 7 **Availability:** Per SAEGW service **Type:** Counter	Int64

Variables	Description	Data Type
saegw-ggsn-subdatastat-dlpktfwd-qci8-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - QCI 8 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci9-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - QCI 9 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci65-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 65 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci66-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 66 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci69-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 69 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci70-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 70 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci80-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 80 on a GGSN (as part of the SAEGW)	Int64
saegw-ggsn-subdatastat-dlpktfwd-qci82-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 82 on a GGSN (as part of the SAEGW)	Int64

Variables	Description	Data Type
saegw-ggsn-subdatastat-dlpktfwd-qci83-64b	The total number of subscriber downlink data packets forwarded on a bearer with a QCI of 83 on a GGSN (as part of the SAEGW)	Int64
saegw-ggsn-subdatastat-dlpktfwd-stdqcinongbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - Std QCI (Non-GBR) **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-stdqcigbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - Std QCI (GBR) **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qcinongbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - Non-Std QCI (Non-GBR) **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-qcigbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - Non-Std QCI (GBR) **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-totgbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - Total GBR **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-dlpktfwd-totnongbr-64b	**Description:** GGSN-anchored Subscriber Data Stats - Downlink packets forwarded - Total Non-GBR **Availability:** Per SAEGW service **Type:** Counter	Int64

Variables	Description	Data Type
saegw-ggsn-subdatastat-ulpktfwd-qci1-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - QCI 1 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci2-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - QCI 2 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci3-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - QCI 3 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci4-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - QCI 4 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci5-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - QCI 5 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci6-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - QCI 6 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci7-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - QCI 7 **Availability:** Per SAEGW service **Type:** Counter	Int64

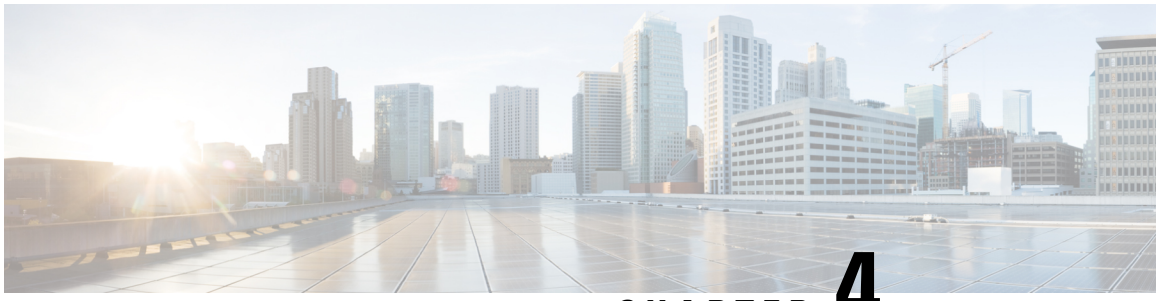
Variables	Description	Data Type
saegw-ggsn-subdatastat-ulpktfwd-qci8-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - QCI 8 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci9-64b	**Description:** GGSN-anchored Subscriber Data Stats - Uplink packets forwarded - QCI 9 **Availability:** Per SAEGW service **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci65-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 65 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci66-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 66 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64
saegw-ggsn-subdatastat-ulpktfwd-qci69-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 69 on a GGSN (as part of the SAEGW) **Type:** Counter	
saegw-ggsn-subdatastat-ulpktfwd-qci70-64b	The total number of subscriber uplink data packets forwarded on a bearer with a QCI of 70 on a GGSN (as part of the SAEGW) **Type:** Counter	Int64

Modified Bulk Statistics

None in this release.

Deprecated Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.27

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.27 software release.

SNMP MIB Alarm Changes for 21.27

There are no new, modified, or deprecated SNMP MIB alarm changes in this release.

SNMP MIB Conformance Changes for 21.27

There are no new, modified, or deprecated SNMP MIB Conformance changes in this release.

SNMP MIB Object Changes for 21.27

This section provides information on SNMP MIB alarm changes in release 21.27.

Important For more information regarding SNMP MIB alarms in this section, see the *SNMP MIB Reference* for this release.

New SNMP MIB Object

This section identifies new SNMP MIB alarms available in release 21.27.

- starSXSelfVersion
- starSRPPeerIpAddress
- starSRPSelfVersion

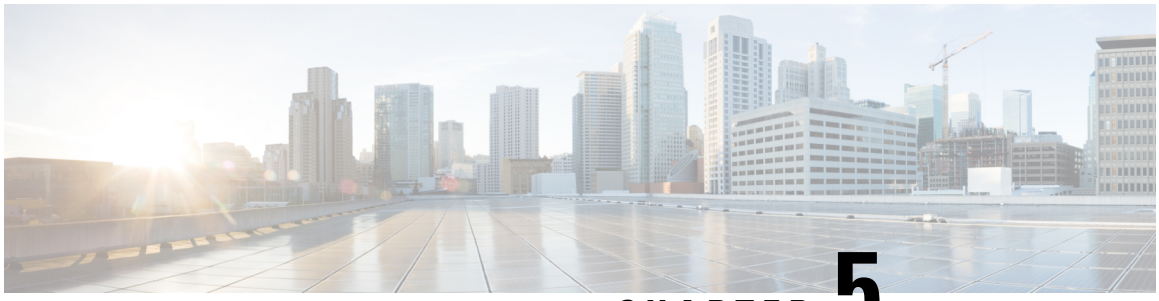
Modified SNMP MIB Object

This section identifies new SNMP MIB alarms available in release 21.27.

- starIPSECTunLocalIpAddr
- starIPSECTunRemoteIpAddr
- starUPlaneTsServiceChainPathNotSelected
- starUPlaneTsServiceChainUp
- starUPlaneTsServiceChainDown
- starUPlaneTsMissConfiguration
- starSxPeerUnsupportedVersion
- starSxPeerUnsupportedVersionClear
- starSRPPeerUnsupportedVersion
- starSRPPeerUnsupportedVersionClear

Deprecated SNMP MIB Object

There are no deprecated SNMP MIB alarm changes in this release.



CHAPTER 5

Addition of Server Unreachable Field in CDR

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	PGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *PGW Administration Guide* • *Statistics and Counters Reference*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
Support is added for addition of server unreachable field in CDR.	21.27

Revision Details	Release
First introduced.	21.22

Feature Description

When the Online Charging System (OCS) sends negative messages, transport connection fails between the Policy and Charging Enforcement Function (PCEF) and the OCS. The connection error causes session establishment failure and prevents subscribers from the use of services. The following procedures are used to overcome the connection errors:

- **Failure Handling (FH)**: The exisiting FH mechanism operates if the diameter session failover is present, allows the system to choose whether to continue the session and convert to offline, or to terminate the session when a connection or message-level error occurs.
- **Server Unreachability (SU)**: This failure handing mechanism provides more granular control over failure procedures. In addition to the session after the message- and connection-level (transport) failures, this mechanism is used when the responses are slow from the OCS. It also provides the options to either continue the session for a specific time duration or quota exhaustion before termination.

  To use the configured server and interim quota (volume and time), SU retries before a session is converted to offline or gets terminated.

When **gtpp attribute servers-unreachable** is configured under gtpp group and the SU feature is enabled then, serversUnreachableContinue or serversUnreachableTerminate in interim or final CDR allows the following process flow:

1. SU failure is triggered.
2. CDR is generated.
3. Based on the SU configuration in Call Control Profile, the generated CDR contains the serversUnreachableContinue or serversUnreachableTerminate fields.

The following table describes the serversUnreachable fields in the CDR.

Table 3: ServersUnreachable Fields in CDR

Field Name	Description	Tag	Format	Size	ASN1 Code
serversUnreachableContinue	When servers unreachable procedure is executed, element is present.	256	Boolean	1	0x9f8200
serversUnreachableTerminate	When servers unreachable procedure is executed, element is present.	257	Boolean	1	0x9f8201

Table 4: ServersUnreachable CDR Fields in ACS Configuration

SU Configuration	SU Detected Fields during Interim State	SU Detected Fields After End of Interim State	SU not Detected Fields (normal call with Gy)

server-unreachable initial-request terminate	When a CDR field is triggered differently, do not include the SU terminate field since it is an interim CDR • **SU continue** is **FALSE** • **SU Terminate** is **FALSE** in final CDR	• **SU continue** is **FALSE** • **SU Terminate** is **TRUE** in final CDR	• **SU continue** is **FALSE** • **SU Terminate** is **FALSE** in final CDR
server-unreachable update-request terminate	When a CDR field is triggered differently, do not include the SU terminate field since it is an interim CDR • **SU continue** is **False** • **SU Terminate** is **False** in final CDR	• **SU continue** is **True** in both interim and final CDR • **SU Terminate** is **False** in final CDR	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR
server-unreachable initial-request continue	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR	• **SU continue** is **True** in both interim and final CDR • **SU Terminate** is **False** in final CDR	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR
server-unreachable update-request continue	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR	• **SU continue** is **True** in both interim and final CDR • **SU Terminate** is **False** in final CDR	• **SU continue** is **False** • **SU Terminate** is **False** in final CDR

For more information, refer to the Gy chapter in the *PGW Administration Guide*.

Adding Server Unreachable Field in CDR

Use the following configuration commands to add the server unreachable field in CDR:

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute servers-unreachable
      end
```

NOTES:

- **gtpp attribute servers-unreachable**: Specifying this option includes the optional field **ServersUnreachablesContinue** or **ServersUnreachablesTerminate** in the CDR.

Monitoring and Troubleshooting

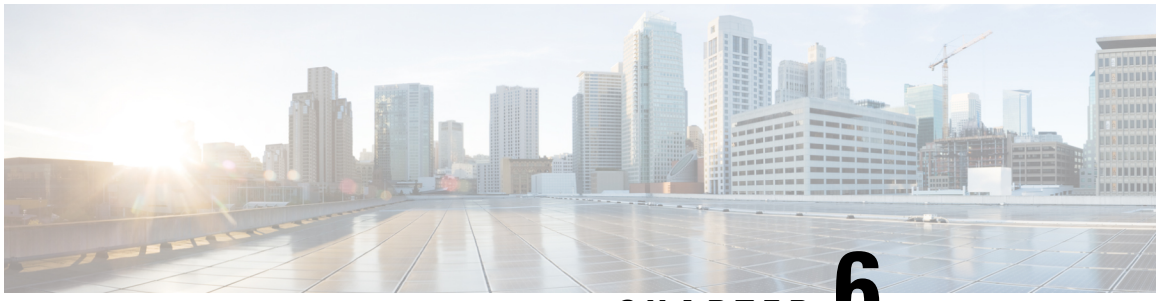
This section provides information to monitor and troubleshoot this feature using show commands.

Show Commands and Outputs

This section provides information regarding show command and their outputs in support of this feature.

show gtpp group name <group name>

Field	Description
Servers Unreachable present	Displays "Yes" or "No" to indicate the presence of servers unreachable element.



CHAPTER 6

Capability to Record and Produce Call Transactions

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• ePDG • P-GW • SaMOG
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide* • *P-GW Administration Guide* • *SaMOG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
P-GW and SaMOG supports capability to record and produce historic call transactions feature. Additional RTT record schemas have been added.	21.27
Added RTT Record Schema	21.26
First introduced.	20.0

Feature Description

Regions and Network Operations Center (NOC) uses Real Time Tool (RTT) to debug network issues and to understand user behavior. All call transactions in ePDG, P-GW, and SaMOG gets generated in RTT files. ePDG, P-GW, and SaMOG transfer RTT files to the external server through SSH File Transfer Protocol (SFTP). The comma-separated values (.CSV) format RTT files get transferred either in compressed or non-compressed format. Transfer happens based on the configuration to the external servers such as servers in the customer network either directly or through the Cisco Collector server.

Note RTT Record Schema and its procedure numbers are generalized for Gateway RTT. Contact your Cisco account representative for detailed information on the specific RTT Record Schema.

How it Works

This section describes the RTT procedures and schema.

RTT Procedures

The following table lists the RTT procedures that are specific to ePDG, P-GW and SaMOG:

Procedure Number	Procedure Name	Applicability
1	S5/S8/S2b GTP Create Session	P-GW, ePDG, SaMOG
2	S5/S8/S2b GTP Create Bearer	P-GW, ePDG, SaMOG
3	S5/S8/S2b GTP Delete Session	P-GW, ePDG, SaMOG
4	S5/S8/S2b GTP Delete Bearer	P-GW, ePDG, SaMOG
5	GTP Modify Bearer	P-GW
6	S5/S8/S2b GTP Update Bearer	P-GW, ePDG, SaMOG
7	S6b/SWm – Diameter AAR/ AAA	P-GW, ePDG, SaMOG

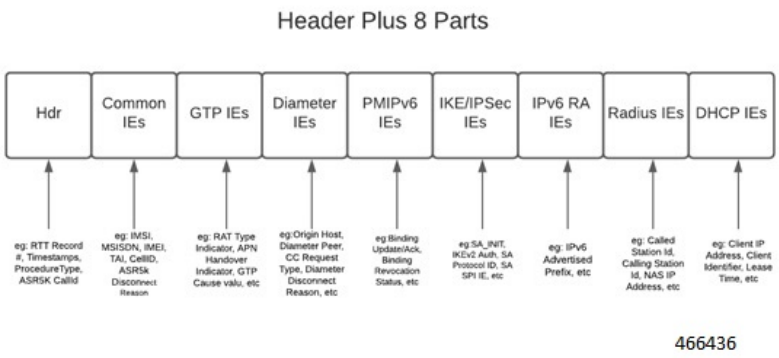
Procedure Number	Procedure Name	Applicability
8	S6b/SWm – Diameter RAR/RAA	P-GW, ePDG, SaMOG
9	S6b/SWm – Diameter Session Termination	P-GW, ePDG, SaMOG
10	S6b – Abort Session	P-GW, ePDG, SaMOG
11	Diameter Gx – CCR-I/CCA-I	P-GW
12	Diameter Gx – CCR-U/CCA-U	P-GW
13	Diameter Gx – CCR-T/CCA-T	P-GW
14	Diameter Gx – RAR/RAA	P-GW
15	Diameter Gy – CCR-I/CCA-I	P-GW
16	Diameter Gy – CCR-U/CCA-U	P-GW
17	Diameter Gy – CCR-T/CCA-T	P-GW
18	Diameter Gy – RAR/RAA	P-GW
19	PMIPv6 S2a – Binding Update/Acknowledgement	P-GW
20	PMIPv6 S2a Revocation Update/Acknowledgement	P-GW
21	SWu – IKEv2 SA INIT/Resp	ePDG
22	SWu – IKEv2 Auth Req/Resp	ePDG
23	SWu – IKEv2 Information Req/Resp	ePDG
24	SWm – Diameter EAP Request/Answer	ePDG, SaMOG
25	ePDG Router Advertisement	ePDG, SaMOG
26	SWu – CREATE_CHILD_SA Req/Resp	ePDG
27	Radius – WLC-SaMOG Access Request/Challenge	SaMOG
28	Radius – WLC-SaMOG Access Request/Accept	SaMOG
29	Radius – WLC-SaMOG Disconnect Request/Response	SaMOG
30	Radius – WLC-SaMOG Accounting Request/Response	SaMOG
31	Radius – SaMOG-Radius Server Accounting Req/Res	SaMOG

Procedure Number	Procedure Name	Applicability
32	WLC – SaMOG DHCP Discover/Offer	SaMOG
33	WLC – SaMOG DHCP Request/Ack/Nak	SaMOG
34	WLC – SaMOG DHCP Release/Ack/Nak	SaMOG

RTT Record Schema

The following figure details the RTT schema for ePDG, P-GW and SaMOG. The first six IEs, Common IEs to IPv6RA IEs are common for ePDG, P-GW and SaMOG. The last two fields, Radius IEs and DHCP IEs are speicific to SaMOG.

Figure 1: RTT Record Schema



RTT schema has a Header followed by eight blocks of Information Elements (IEs). There are 220 IEs that are grouped into 8 blocks. Schemas 1 to 170 are specific to ePDG. Schemas 1 to 170 + 10 (180) CUPS schemas are specific to P-GW and schemas 171 to 220 are specific to SaMOG. For more information on CUPS schemas, refer to the *Ultra Packet Core CUPS User Plane Administration Guide*. Contact your Cisco account representative for the complete list of RTT Record Schema IEs.

The following table lists the RTT Record schemas:

IE	Description	Format Example	Relevant Procedures
1	Gateway RTT Record Number	Counter in <proclet-type> | <instance-id> | <RTT-record-#>	All
2	Gateway RTT Version Number	Version 3 in R20.0	All
3	Procedure Number	Defined in CFS Table 1	All
4	Gateway Name	Host Name of the Chassis	All
5	Procedure Start Time (GMT)	Time in UTC, (to ms accuracy)	All
6	Procedure End Time (GMT)	Time in UTC, (to ms accuracy)	All

IE	Description	Format Example	Relevant Procedures
7	ASR5K CallID	Internal CallID, for example [376efb10]	All
8	GW Name	Gateway name (ePDG/P-GW/SaMOG) for which the RTT record is generated.	All
9 to 10	Reserved		
11	IMSI	Example [311480076488840]	1, 11, 12, 13, 22, 24, 27, 28, 30, 32, 33 and 34
12	MSISDN	Example [19728256305]	1, 5, 7, 15, 16 and 17
13	IMEISV	Example [9900028823793406]	1, 11 and 15
14	TAI - MCC/MNC/TAC	Example string [311-480-0x3B00]	1 through 6 ,11, 12, 15 and 16
15	Cell ID	ECI. Example [0xE70D01]	1 through 6, 11, 12, 15 and 16
16	ASR5.5K Disconnect Reason	Internal reason for session disconnect (Example: timeout, error). For more information, refer to the *Statistics and Counters Reference Guide.*	All (pending error)
17	MAC Address	MAC address of the UE device. This attribute is same as the calling-station-ID, in case of SaMOG radius call flow. Example: 0034567890AB	24, 27, 28, 29, 30, 31, 32, 33 and 34
18 to 20	Reserved		
21	Serving Network	MCC MNC. Example [311480]	1 and 5
22	Radio Access Technology	Defined in TS29.274, example [6 = E-UTRAN]	22
23	Handover Indicator	HI field in Indication attribute; example [0 = New PDN; 1 = Handover]	1 and 5
24	SGW/HSGW/ePDG/SaMOG Control TEID	Tunnel Identifier for Peer. Example [0x26B609F0]	1, 2 and 5
25	PGW Control TEID	Tunnel Identifier for PGW. Example [0x084BC005]	1 and 2

IE	Description	Format Example	Relevant Procedures
26	AN GW Address	IP Address of Remote GW: HSGW or SGW	1, 2 and 5
27	Access Point Name	String, example: [Customerims.mnc311.mcc480.3gppnetwork.org]	1
28	Framed-IP Address	UE assigned IPv4 address	1, 11, 12 and 13
29	Framed-IPv6 Address	UE assigned IPv6 prefix/address	1, 11, 12 and 13
30	Uplink AMBR	In Kbps; example [0-4294967295]	1 and 6
31	Downlink AMBR	In Kbps; example [0-4294967295]	1 and 6
32	PCO DNS IPv6 Address – Primary	IPv6 Address of Primary DNS server	1
33	PCO DNS IPv6 Address – Secondary^Tertiary	Secondary IPv6 Address ^ Tertiary IPv6 Address for DNS	1
34	PCO DNS IPv4 Address – Primary	IPv4 address	1
35	PCO DNS IPv4 Address - Secondary	Secondary IPv4 Address ^ Tertiary IPv6 Address for DNS	1
36	List of EPS Bearer IDs (Successful	Each bearer Id shall be separated by a “|” Example 1 | 3 | 5	1, 2, 4, 5 and 6
37	Linked Bearer Identity	Based on TS29.274, example [0-15]	2, 3, 4 and 5
38	Uplink MBR	In Kbps. MBR. Example 1234 | 3456 | 567 MBR of each bearer shall be separated by "|” and has the same order as of IE 37	1 and 6
39	Downlink MBR	Same as Uplink MBR	1 and 6
40	Uplink GBR	In Kbps. GBR. Example 1234 | 3456 | 567 MBR of each bearer shall be separated by "|” and has same order as of IE 37	1 and 6
41	Downlink GBR	Same as Uplink GBR	1 and 6

IE	Description	Format Example	Relevant Procedures
42	GTP Cause Value	Based on TS29.274 Request/Acceptance/Rejection Cause, example [1-255]	1 to 6
43	Piggyback Record Indicator	Explicit indication of piggyback message record, example (0=no; 1=yes)	2 and 5
44	Reserved		
45	SGW/HSGW/ePDG/SaMOG Data TEID	Tunnel Identifier for Peer, example [0x26B609F0]	1,2 and 5
46	PGW Data TEID	Tunnel Indentifier for P-GW, example [0x084BC005]	1 and 2
47 to 50	Reserved		
51	Session ID	Session-ID for Authentication Session, example, UTF8 String [0006-diamproxy.WSBOMAGJPNC.S6b.vzims.com; 21604107; 449305093; 536f9359-503]	7 to 18 and 24
52	Auth-Application ID	Example [S6b = 16777999 , Gx = 16777238, Gy = 4]	7 to 18 and 24
53	PGW-Host (Origin Host)	FQDN of PGW, example [0004-diamproxy. WSBOMAGJPNC. Gy.vzims. com]	7 to 18 and 24
54	Diameter Peer Address Realm	FQDN of 3GPP AAA, PCRF OCS realm, example [Customerims.com]	7 to 18 and 24
55	Dest Peer Host	FQDN of 3GPP AAA, PCRF, OCS host, example [njbbpcrf1a.vzims.com]	7 to 18 and 24
56	CC Request Type	Example Enumerated [1-3, for I, U, T]	11, 12, 13, 15, 16 and 17
57	CC Request Number	Example [0]	11, 12, 13, 15, 16 and 17
58	Result Code	Diameter Result Code based on RFC3588, example [2001]	7 to 18 and 24
59	Origin State ID	Example [1366695723]	7 to 18

IE	Description	Format Example	Relevant Procedures
60	Service-Selection	AVP used for providing APN name for authorization, example [Customerinternet]	12 and 24
61	Charging Gateway Function Host	FQDN of CGF, example [cgf1.NEE29.vzims.com]	5 and 7
62	Charging Group ID	Charging ID of each bearer shall be separated by "|" in the order same as that of IE 37 followed by 44	5 and 7
63	Server-Name (CSCF Address)	Only on IMS APN, example [pcscf1.CTX07.vzims.com]	7
64	Framed-pool	Pool name from which IPv4 address is to be allocated, example [int41]	7
65	Framed-IPv6-Pool	Pool name from which IPv6 prefix is to be allocated, example [ims61]	7
66	Auth-Request-Type	Based on TS29.273 and 29.212. Example Enumerated [1-3]	7 and 24
67	Re-Auth-Request-Type	Based on TS29.273 and 29.212. Example Enumerated [0-1]	8, 14 and 18
68	Diameter Termination Cause	Based on TS29.273 and 29.212. Example Enumerated [1-8]	9, 13 and 17
69	QoS Class Identifier	QCI, example [8]	11, 12, 15 and 16
70	IP-CAN Type	Example [5 = 3GPP-EPS]	11, 12 and 14
71	Event Trigger	Based on TS29.212, Series of Pipe Delimited Triggers, example [1 = QOS_CHANGE]	11 and 12
72	Reserved IE / Unused		
73	Charging-Rule-Remove	Name of the removed Charging rule, example String [RTRRule3300]	12
74	Charging-Rule-Install	Name of the installed Charging rule, example String[RTRRule3300]	11
75	Multiple Services Indicator	Based on TS32.299, example Enumerated [0-1]	15, 16 and 17

IE	Description	Format Example	Relevant Procedures
76	Multiple Services Credit Control Rating-Group	Identifier of Rating Troup, example [3300]	15, 16 and 17
77	Multiple Services Credit Control Granted Service Unit	CC-Total-Octets, example [524288000]	15
78 to 80	Reserved		
81	EAP Auth-Session-State	Example: STATE_MAINTAINED (0)	24
82	WLAN User-Name	Example: 0311150123456701@ wlan.mnc150. mcc311.3 gppnetwork.org	24
83	RAT Type	Example: 0 = WLAN	24
84	Visited Network Identifier	Example: mnc150.mcc311.3gppnetwork.org	24
85	EAP-Master-Session-Key	MSK	24
86	APN Configuration	PDN-Type | Service = Selection | Gateway	24
87 to 90	Reserved		
91	MAG IP Address	MAG IP Address	19 and 20
92	LMA IP Address	LMA IP Address	19 and 20
93	IMSI-NAI	Example:. 6311480000021024@nai.epc. mnc480. mcc311.3 gppnetwork.org	19 and 20
94	Service Selection Mobility Option	Set to EPS APN Name, formatted as 3GPP TS 23.003, example, Customerims	19 and 20
95	Home Network Prefix Option	Dynamic or Static Prefix assigned plus IID allocated for UE	19 and 20
96	IPv4 Address Request	Address/Prefix, example. 209.165.200.225/32	19
97	IPv4 Address Acknowledgement	Status:Address/Prefix, example. 0:209.165.200.225/32	19
98	IPv4 Default Router	IPv4 Address, example. 209.165.200.226	19

IE	Description	Format Example	Relevant Procedures
99	Uplink GRE key	Hex, e.g. 0x004D90CC	19
100	Downlink GRE key	Hex, example. 0xCC904D00	19
101	Charging Characteristics	Hex, example. 0x0A	19
102	Charging ID	Hex, example. 0x5E9BD665	19
103	Serving Network	MCC-MNC	19
104	Base Station ID	Hex, example. 001C0001008A	19
105	MEID	Decimal String, example. 99000044001930	
106	Binding Sequence #	16 bit unsigned integer for Binding Update and Ack	19
107	Lifetime	16 bit unsigned integer representing ime before binding unit is considered expired. Example. 0x0708	19
108	Handoff Indicator Option	HO Indicator Example. 0x01 = new attachment	19
109	Access Technology Type (ATT)	Example. 0x09 = eHRPD	19
110	Proxy Binding Status	8-bit unsigned integer indicating status of BU processing.	19
111	PCO DNS IPv6 Address	DNS IPv6 Address. if multiple, format = “Addr1|Addr2”	19
112	PCO DNS IPv4 Address	DNS IPv4 Address. if multiple, format = “Addr1|Addr2”	19
113	P-CSCF Address	P-CSCF IPv6 Address (if multiple, format = “Addr1!Addr2”	19
114	Binding Revocation Status	8-bit unsigned integer indicating result of processing BRI. Values less than 128 indicates success	20
115	Binding Revocation Sequence #	Sequence number to match BRI and BRA messages	20
116	Revocation Trigger	8-bit unsigned integer indicating per UE or global reasons for trigger	20

IE	Description	Format Example	Relevant Procedures
117	Revocation Flag	Hex, example. 0x4	20
118 to 130	Reserved		
131	UE IP Address	UE IP address	21, 22, 23 and 26
132	UE UDP Port for SA_INIT	UE UDP Source Port for SA_INIT	21, 22, 23 and 26
133	ePDG Address	ePDG IP address for SA_INIT	21, 22, 23 and 26
134	ePDG Port	ePDG UDP Port for SA_INIT (example: 4500 for IKE)	21, 22, 23 and 26
135	Initiator SPI	Initiator (UE) SPI	21, 22 and 26
136	Responder SPI	Responder (ePDG) SPI	21, 22 and 26
137	Transform Header Type and ID	TypeID negotiated value is entered. x|y|z|w|U (Enc/prf/Integrity/Dhg/ESN) In case value is not negotiated, then -1 is entered. Example: PRF is not present in IKE_Auth. Value will be IANA standard number for these protocols.	21, 22 and 26
138	KE DH Group	Diffie Hellman Group Number	21 and 26
139	Notify Message Type	Example: NAT_Detection IP Type (delimited as necessary) will be delimited as x|y|z^a|b|c where x/y/z are notify in Procedure request and a/b are notify in Procedure response. If either Request or Response doesn't have any Notify, it will be blank either before or after the delimiter ^.	21 and 26
140	IDi	Identification Initiator: RFC822 Address, example: 0311150123456701@wlan.mnc150. mcc311. 3gppnetwork.org	22
141	IDr	Identification Responder: IKEv2 FQDN ID, example: apncf.w-apn. mnc150.mcc311. pub. 3gppnetwork.org	22

IE	Description	Format Example	Relevant Procedures
142	TSi	Protocol Type|Address Range|Port Range (Can be delimited by ^ if more than one TS)	22
143	TSr	Protocol Type|Address Range|Port Range (Can be delimited by ^ if more than one TS)	22
144	EAP Message Status Code	Example:. SUCCESS This will assume last value in the response	22, 27 and 28
145	EAP Message Identifier	EAP Message Identifier	22 and 27
146	EAP Type	Example: AKA (0x17) for ePDG EAP-AKA (0x17)	22, 27 and 28
147	Configured Attribute Auth Method	Shared Key as String. Example: local_method|remote_method where local/remote could be PSK/EAP/CERT	22
148	IKEv2 Config Attribute Internal IP4/IPv6	Example: UE address x^y where x is IPv4 and y is IPv6	22
149	IKEv2_CFG_ ATTRIBUTE_INTERNAL_ IP4_NETMASK	Example: 255.255.255.255	22
150	IKEv2_CFG_ ATTRIBUTE_ INTERNAL_DNS_ IPV4	x^y^z where x,y,z will be IPv4 address. Maximum of 3 entries possible in IKE_Auth_reply.	22
151	IKEv2_CFG_ ATTRIBUTE_ INTERNAL_DNS_ IPV6	x^y^z where x,y,z will be IPv6 address. Maximum of 3 entries possible in IKE_Auth_reply. This IE is missing. New one needs to be added	22
152	P-CSCF IPv4	x^y^z where x,y, z will be IPv4 address. Maximum of 3 entries possible in IKE_Auth_reply.	
153	P-CSCF IPv6	x^y^z where x,y,z will be IPv6 address. Maximum of 3 entries possible in IKE_Auth_reply.	22
154	SA Protocol ID	Example: ESP (0x03)	22

IE	Description	Format Example	Relevant Procedures
155	SA SPI UE	Example: 0x020000BA	22
156	SA SPI ePDG	Similar to SA SPI UE. This is missing. Needs to be added	
157	Informational Request Type	Delete, DPD, and so on.	23
158	IKEv2 Notify – Error Codes	Reference IKEv2 standard Error Codes and Customer Custom Codes per SWu Call Flow: Finally received /sent Notify error code is updated. This could be the Verison custom code if configured, or standard code otherwise.	21, 22, 23 and 26
159 to 160	Reserved		
161	IPv6 Advertised Prefix	Advertised IPv6 Prefixes as part of Router Advertisement	25
162 to 170	Reserved		
171	Called -Station-ID	Stores the bridge or Access Point MAC address in ASCII format with octet values separated by a "-" appended by SSID. Example:: mac64-d9-89-43- d4-a0: grp123456789123456789	27, 28, 30 and 31
172	Service-Type	Indicates the type of service the user has requested, or the type of service to be provided. Example: 02 (Framed).	27, 28, 30 and 31
173	NAS-Port-Type	Indicates the type of the physical port of the NAS which authenticates the user. Example: 19 (Wireless_IEEE_802_11)	27, 28, 30 and 31
174	NAS-Port-ID	Identifies the port of the NAS which authenticates the user. Example: 10	27, 28, 30 and 31
175	NAS-IP-Address	Indicates the identifying IP Address of the NAS which requests user authentication. Example: 192.168.15.51	27, 28, 29, 30 and 31

IE	Description	Format Example	Relevant Procedures
176	NAS-IPv6-Address	Indicates the IP Address of the NAS which requests user authentication.Example: 2405:200:816:945::2:ed9e	27, 28, 29, 30 and 31
177	NAS-Identifier	Indicates a string identifying the NAS origination the request. Example: samog_wlc	27, 28, 29, 30 and 31
178	Acct-Session-ID	Indicates the session to match start and stop records in a log file.	27, 28, 29, 30 and 31
179	Acct-Multi-Session-ID	Indicates a unique Accounting ID to link multiple related sessions in a log file. Each session linked together would have a unique Acct-Session-Id but the same Acct-Multi-Session-Id.	27, 28, 29, 30 and 31
180	NAS-Port	Indicates the physical port number of NAS, which authenticates the user. Example: 1	27, 28, 30 and 31
181	Framed-MITU	Indicates the maximum transmission unit to be configured for the user. Example: 1300	27 and 28
182	Reserved		
183	Framed-IP-Address	Indicates the address allocated for the user. Example: 1,2,3,5	29, 30 and 31
184	Acct-Termination_Cause	Indicates the session termination cause. Example: 1 for user request.	29
185	Framed-IPv6-Prefix	Indicates the IPv6 prefix for the user. Example: 1:2:3:5::/64 or 1:2:3:5::	29, 30 and 31
186	Tunnel-Type	Indicates the tunneling protocol. Example: 14 for VLAN.	27, 28, 30 and 31
187	Tunnel-Medium-Type	Indicates the transport medium for creating protocol. Example: 06 for IEEE-802	27, 28, 30 and 31

IE	Description	Format Example	Relevant Procedures
188	Tunnel-Private-Group-ID	Group ID for the specified tunneling session	27, 28, 30 and 31
189	Acct-Output-Packets	Number of packets sent. Example: 20	30 and 31
190	Acct-Input-Packets	Number of packets received. Example: 24	30 and 31
191	Acct-Status-Type	Indicates the beginning or end of user service. Example 1 (start) 2 (stop).	30 and 31
192	Acct-Session-Time	Indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.	30 and 31
193 to 205	Reserved		
206	Transaction ID	Transaction ID. Example: 0x7df10d5d	32 and 33
207	Client IP Address	The IP address alloted to the client through the address: 13.0.0.2	32, 33 and 34
208	Requested IP Address	IP Address requested by the client in DHCP Request message. (DHCP Option: requested ip addr(50) : 13.0.0.2	33
209	Default GW	Default Gateway IP Address. Example: DHCP Option - default gateway(03) : 25.8.0.1	32 and 33
210	Primary DNS Server	Primary DNS Server IP Address. Example: DHCP Option - primary dns server(06) : 49.45.0.1	32 and 33
211	Secondary DNS Server	Secondary DNS Server IP Address. Example: DHCP Option - secondary dns server(06) : 4.5.6.7	32 and 33
212	Lease Time	Lease time's IP address. Example: DHCP Option - lease time(51) : Infinite / 2000 in seconds	32 and 33

IE	Description	Format Example	Relevant Procedures
213	Server identifier	DHCP Server Identifier . Example: DHCP Option - server identifier(54) : 10.70.150.223	32 and 33
214	Subnet Mask	Subnet mask IP address. Example: DHCP Option - subnet mask(01) : 255.255.0.0	32 and 33
215	Error Message	Example: DHCP Option-message (56) : Invalid requested IP	33 and 34
216 to 220	Reserved		

Note Schemas 1 to 170 are speicific to ePDG. Schemas 1 to 170 + 10 Cups schemas are specific to PGW and schemas 171 to 220 are specific to SaMOG.

Configuring RTT

This section provides RTT configuration information for ePDG, P-GW and SaMOG.

Configuring RTT to Record and Produce Call Transactions

Use the following configuration to enable RTT to record and produce call transactions.

```
configure
   context context_name
      [ epdg-service | pgw-service | samog-service ] service_name
         [ no ] reporting-action event-record
end
```

NOTES:

- **reporting-action event-record**: Enables event reporting through RTT.
- **no**: Disables event reporting through RTT.

Configuring RTT under Session Event Module

Use the following configuration to configure the RTT feature in ePDG, P-GW and SaMOG.

```
configure
   context context_name
      session-event-module
```

```
        event transfer-mode push primary url URL_addressfile name file_name |
 rotation volume volume_size | rotation time rotation_time | compression
compression_type | extension extension_type
        event use-harddisk
        event remove-file-after-transfer
        event push-interval interval_time
      end
```

NOTES:

- **transfer-mode**: Enables the transfer mode in RTT.
- **push primary url***URL_address*: Specifies the external server location where the records are transferred.
- **file name** *file_name*: Specifies the RTT file name where the records are stored. *file_name* can be an alphanumeric string of size 1 to 31.
- **rotation volume** *volume_size*: The volume based on which the RTT file is generated. Enter an integer from 51200 to 62914560.
- **rotation time** *rotation_time*: The time based on which the RTT file is generated. Enter an integer from 30 to 86400 seconds.

  Note RTT files are internally generated, based on the rotation volume or rotation time.

- **compression**: Specifies the file compression type. If enabled, the RTT file is generated as a Gzip file, else it is generated as a normal file.
- **extension***extension_type*: Specifies the RTT file extension (.csv).
- **event use-harddisk**: Specifies hard disk as the storage space for the RTT file generation.
- **event remove-file-after-transfer**: Specifies RTT files to be removed after pushing the files to the external server.
- **event push-interval**: Specifies the push interval time at which the RTT files are transferred to the external server.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands to support this feature.

Show Commands and Output

This section provides information regarding show commands and their outputs for this feature.

show samog-service name

Table 5: show samog-service name Command Output Descriptions

Field	Description
Reporting Action	
Event Record	Indicates if RTT feature is enabled or not.

show event-record statistics

Table 6: show event-record statistics Command Output Descriptions

Field	Description
Total Number of Event Records	The total number of event records (GTPv2 + Diameter + IKE + RA + Radius + DHCP).
GTPv2 Event Records	The total number of GTPv2 records
CSR	The total number of CSR (Create Session Request) events.
CBR	The total number of CBR (Create Bearer Request) events.
DSR	The total number of DSR (Delete Session Request) events.
DBR	The total number of DBR (Delete Bearer Request) events.
UBR	The total number of UBR (Update Bearer Request) events.
IPV6 RA Event Records	The total number of IPV6 RA event records.
RA Prefix	The total number of RA prefix events.
Diameter Event Records	The total number of Diameter event records (S6b + SWm + STa + Gx + Gy).
ePDG Events	
IKEv2 Event Records	The total number of IKE events.
IKE_SA_INIT	The total number of IKE_SA_INIT events.
IKE_AUTH	The total number of IKE_AUTH events.
IKE_INFORMATION	The total number of IKE_INFORMATION events.
CREATE_CHILD_SA	The total number of CREATE_CHILD_SA events.
SaMOG Events	
Radius Auth Event Records	The total number of Radius authentication event records.

Field	Description
Access Req/Challenge	The total number of Radius Authentication access request challenge event records.
Access Req/Accept	The total number of Radius Authentication access request accept event records.
Disconnect Req	The total number of Radius Authentication disconnect request event records.
Radius Accounting Event Records	The total number of Radius accounting event records.
Accounting Req from WLC	The total number of Radius accounting event records from WLC.
Accounting Req to Radius Server	The total number of Radius accounting event records to the Radius server.
STa Procedures	The total number of STa interface specific events.
AAR	The total number AAR (AA-Request) events.
RAR	The total number of RAR (Re-Auth-Request) events.
ASR	The total number of ASR (Abort Session Request) events.
STR	The total number of STR (Session Termination Request) events.
DER	The total number of DER (DE-Request) events.
DHCP Event Records	The total number of DHCP event records.
Discover/Offer	The total number of DHCPv4 discovery offer event records.
Release/Ack	The total number of DHCPv4 release ack event records.
Request/Ack	The total number of DHCPv4 request ack event records.

Bulk Statistics

The following bulk statistics are added to the SaMOG schema as part of this feature:

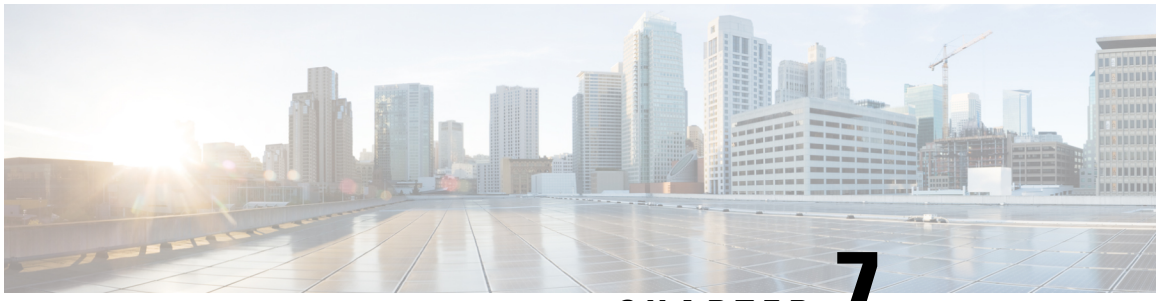
SaMOG Schema

Table 7: Bulk Statistics Varibales in the SaMOG Schema

Variables	Description
sess-samog-total-number-event-records	The total number of SaMOG session event records.
sess-samog-total-s2a-event-records	The total number of SaMOG S2a event records.
sess-samog-total-csr-event-records	The total number of SaMOG CSR event records.

Variables	Description
sess-samog-total-cbr-event-records	The total number of SaMOG CBR event records.
sess-samog-total-dsr-event-records	The total number of SaMOG DSR event records.
sess-samog-total-dbr-event-records	The total number of SaMOG DBR event records.
sess-samog-total-ubr-event-records	The total number of SaMOG UBR event records.
sess-samog-total-ipv6-ra-event-records	The total number of SaMOG IPv6 RA event records.
sess-samog-total-ra-prefix-event-records	The total number of SaMOG RA prefix event records.
sess-samog-total-dhcpv4-event-records	The total number of SaMOG DHCPv4 event records.
sess-samog-total-dhcpv4-disc-offer-event-records	The total number of SaMOG DHCPv4 discovery offer event records.
sess-samog-total-dhcpv4-req-ack-event-records	The total number of SaMOG DHCPv4 request acknowledgement event records.
sess-samog-total-dhcpv4-rel-ack-event-records	The total number of SaMOG DHCPv4 release acknowledgement event records.
sess-samog-total-rad-auth-event-records	The total number of SaMOG Radius Authentication event records.
sess-samog-total-rad-auth-acc-req-chal-event-records	The total number of SaMOG Radius Authentication access request challenge event records.
sess-samog-total-rad-auth-acc-req-acpt-event-records	The total number of SaMOG Radius Authentication access request accepted event records.
sess-samog-total-rad-auth-disc-req-event-records	The total of number SaMOG Radius Authentication disconnect request event records.
sess-samog-total-rad-acct-event-records	The total number of SaMOG Radius Accounting event records.
sess-samog-total-rad-acct-wlc-event-records	The total number of SaMOG Radius Accounting event records from Wireless LAN Controller.
aaa-samog-total-rad-acct-aaa-event-records	The total number of SaMOG Radius Accounting event records to AAA.
aaa-samog-total-sta-event-records	The total number of SaMOG STa event records.
aaa-samog-total-sta-aar-event-records	The total number of SaMOG STa AAR event records.
aaa-samog-total-sta-der-event-records	The total number of SaMOG STa DER event records.
aaa-samog-total-sta-asr-event-records	The total number of SaMOG STa ASR event records.
aaa-samog-total-sta-rar-event-records	The total number of SaMOG STa RAR event records.

Variables	Description
aaa-samog-total-sta-str-event-records	The total number of SaMOG STa STR event records.



CHAPTER 7

Cloud Initialization Support for Elastic Services Controller

Feature Summary and Revision History

Summary Data

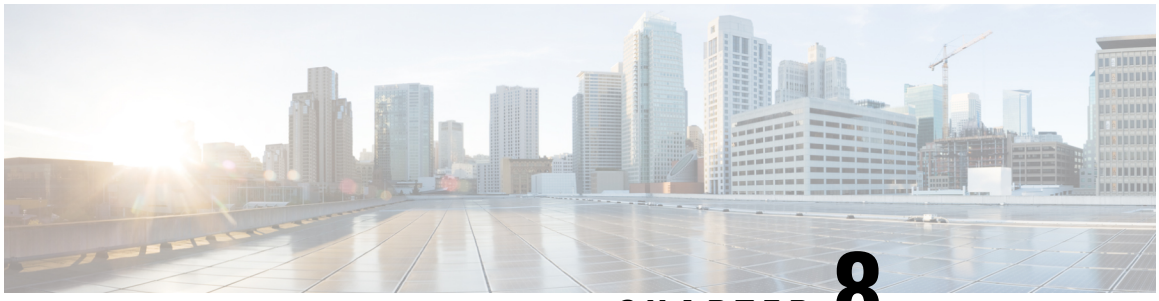
Applicable Product(s) or Functional Area	StarOS
Applicable Platform(s)	VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Openstack 16 and above
Related Documentation	*ASR 5500 System Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.27

Feature Description

When Elastic Services Controller (ESC) uses Cinder Multi-Attach volume on Control Function (CF), Active and Standby for QvPC-DI, the invoked Openstack API version for virtual machine (VM) Orchestration is 2.60 or higher. In this API version, ESC encodes and injects the configuration files into the VM for security reasons. Since, the VM is unable to read the encoded configuration files, ESC uses the **`user_data`** compressed file. This **`user_data`** file contains the configuration files that are required to boot VM.



CHAPTER 8

Customizing Access-Link IP Fragmentation

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Support is added for access-link fastpath to enforce APN MTU for IPv4 traffic.	21.27
First introduced.	21.26

Feature Description

The P-GW APN level configuration controls the IP fragmentation, if the forward or drop logic for IP packets that are larger than MTU, becomes higher due to GTPU encapsulation overheads. To override multiple configurations at the APN level, the global-level CLI reduces deployment time, configuration size, and minimizes errors.

Note If the CLI is not configured at the APN level, the Global level configuration is applied by default. If the CLI is not configured at the Global level, then the default value is applied.

Configuring Access-Link IP Fragmentation

Configuring access-link IP fragmentation involves the following steps:

- Configuring Global Level Access-Link IP Fragmentation
- Configuring APN Level Access-Link IP Fragmentation
- Configuring Access-Link Fastpath to Enforce APN MTU

Configuring Global Level Access-Link IP Fragmentation

Use the following configuration to configure the access-link IP fragmentation in the Global configuration mode:

```
configure
  [ default ] access-link ip-fragmentation { df-fragment-and-icmp-notify
 | df-ignore | normal }
  end
```

NOTES:

- **access-link ip-fragmentation**: Configures the access-link IP fragmentation to the mobile node if the link MTU is smaller than the packet length.
- **df-fragment-and-icmp-notify**: Partially ignores the DF bit setting when the packet is fragmented. It also sends ICMP unreachable error to the source, even if DF bit is set for the packet.

- **df-ignore**: Ignores the DF bit setting when the packet is fragmented. This is the default value.
- **normal**: Configures the normal fragmentation process.
- **default**: The default value is set to **df-ignore**.

Configuring APN Level Access-Link IP Fragmentation

Use the following configuration to configure the access-link IP fragmentation in the APN configuration mode:

```
configure
   context context_name
      apn apn_name
         [ no ] access-link ip-fragmentation { df-fragment-and-icmp-notify
 | df-ignore | normal }
         end
```

Note The **no** option is introduced in the APN configuration and the **default** option is deprecated.

NOTES:

- **access-link ip-fragmentation**: Configures the access-link IP fragmentation to the mobile node if the link MTU is smaller than the packet length.
- **df-fragment-and-icmp-notify**: Partially ignores the DF bit setting when the packet is fragmented. It also sends ICMP unreachable error to the source, even if DF bit is set for the packet.
- **df-ignore**: Ignores the DF bit setting when the packet is fragmented.
- **normal**: Configures the normal fragmentation process.

Configuring Access-Link Fastpath to Enforce APN MTU

The downlink SGi IP packet may get fragmented before it is sent out through the GTP tunnel. The packet is not fragmented, if the packet size and GTP tunnel encapsulation is smaller than or equal to the APN MTU size. If the packet size and GTP tunnel encapsulation are bigger than the APN MTU size, then the packet is fragmented before it is sent through the GTP tunnel. The packet is fragmented either in the inner or outer packet. The global-level configuration enforces the VPP enabled platform to perform outer packet fragmentation upon receiving the nonfragmented packets.

Use the following configuration to access-link fastpath to enforce APN MTU for IPv4 traffic:

```
configure
   [ no ] access-link fastpath apn-ppp-mtu-enforce
   end
```

NOTES:

- **access-link fastpath apn-ppp-mtu-enforce**: Enforces the APN MTU to VPP-based fastpath IPv4 data streams.

Note After configuration, the newly created bearers are set to the newly configured value. However, the ongoing bearer traffic does not get affected due to this configuration. The **access-link fastpath apn-ppp-mtu-enforce** is disabled by default and is not supported in the VPC-DI platform.

Monitoring and Troubleshooting

This section provides information regarding show commands and their outputs.

Show Commands and Output

This section provides information regarding show commands and their outputs in support of this feature.

show configuration access-link

The output of this command displays the following field.

Field	Description
access-link ip-fragmentation normal	Displays the respective value, if configured at Global level. If the configuration is set to **default** or **df-ignore** then, no output is displayed.

show configuration access-link verbose

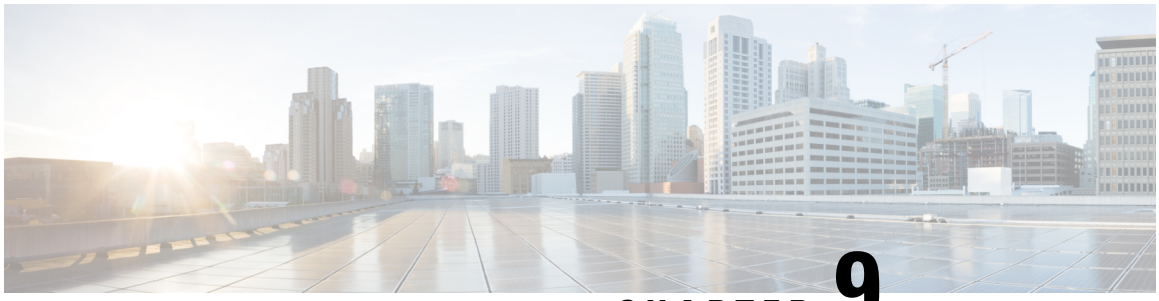
The output of this command displays the following field.

Field	Description
access-link ip-fragmentation df-ignore	Displays the respective value, if configured at Global level. If the configuration is set to **default** or **df-ignore** then, df-ignore is displayed.

show config apn <apn_name>

The output of this command displays the following field.

Field	Description
access-link ip-frag: df-ignore (APN-Configured: False)	Displays the application logic applied to the APN. APN-Configured confirms if the application logic is derived from the APN (True) or from the Global level (False).



CHAPTER 9

Configuring SRP Checkpoint

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ASR 5500
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *ASR 5500 System Administration Guide* • *Command Line Interface Reference* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
VRF configuration under the BGP router configuration is supported in SRP checkpoint functionality.	21.27.m0

Feature Description

Interchassis Session Recovery (ICSR) setup requires some configurations to be identical on both the active and standby chassis. Service Redundancy Protocol (SRP) Checkpoint or Checksum validates the configurations on the active and the standby chassis, and if they are identical, then the configurations are correct. If the configurations are not identical, then errors can occur. VRF configurations are added under BGP router configuration to support SRP Checkpoint.

Configuring SRP Checkpoint

Use the following configuration to configure SRP Checkpoint.

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bgp vrf-srp-validate
      end
```

NOTES:

- **vrf-srp-validate**: Enables SRP validation for BGP VRF configuration.
- **no**: Disables SRP validation for BGP VRF configuration.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands to support this feature.

Show Commands and Output

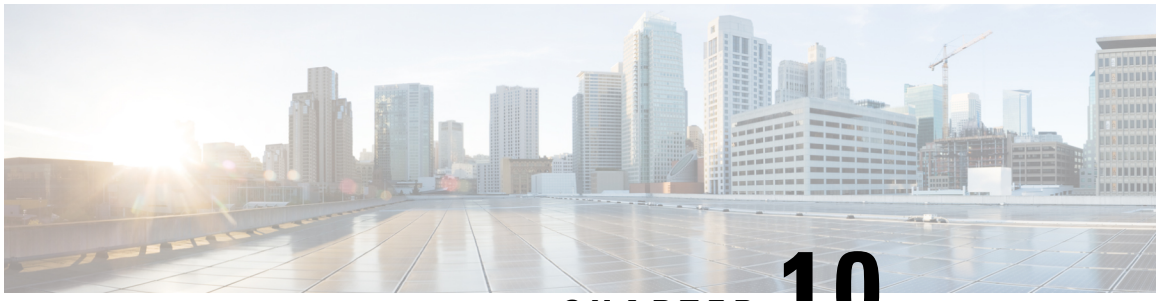
This section provides information regarding show commands and their outputs for this feature.

show configuration srp

The output of this command is enhanced to display the following field.

Table 8: show configuration srp Command Output Descriptions

Field	Description
vrf-srp-validate	Enables the SRP validation for BGP VRF configuration.



CHAPTER 10

Deprecated CLI for MME Initiated PDN Disconnection

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*Command Line Interface Reference*

Revision History

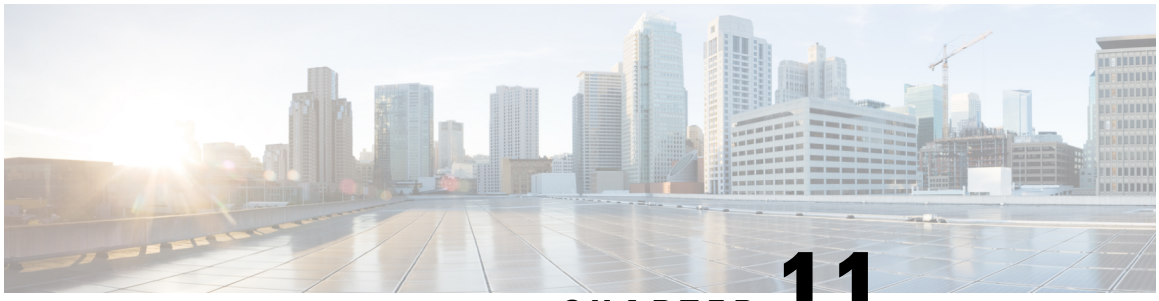
Revision Details	Release
First introduced.	21.27.2

Feature Changes

Previous Behavior: The existing CLI, **clear subscriber mme-service** *service_name* **ebi** *id* performs MME initiated PDN disconnection for the PDNs with ebi number mentioned.

New Behavior: The CLI **clear subscriber mme-service** *service_name* **ebi** *id* is deprecated as there is no usage for long time.

Note The deprecated message is displayed while using the CLI **clear subscriber mme-service** *service_name* **ebi** *id*.



CHAPTER 11

Enable mme clear-route-multipath-zero in CLI

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*Command Line Interface Reference*

Revision History

Revision Details	Release
The test CLI **mme clear-route-multipath-zero mme-service** *service_name* **enable/disable** is removed from Exec mode and the new CLI **clear-route-multipath-zero** is configured under mme-service.	21.27.0

Feature Changes

Previous Behavior: The existing test CLI, **mme clear-route-multipath-zero mme-service** *service_name* **enable/disable** was configured under Exec mode.

New Behavior: The new CLI, **clear-route-multipath-zero** is configured under mme-service Config mode.

Note The existing test CLI is removed from the Exec mode.

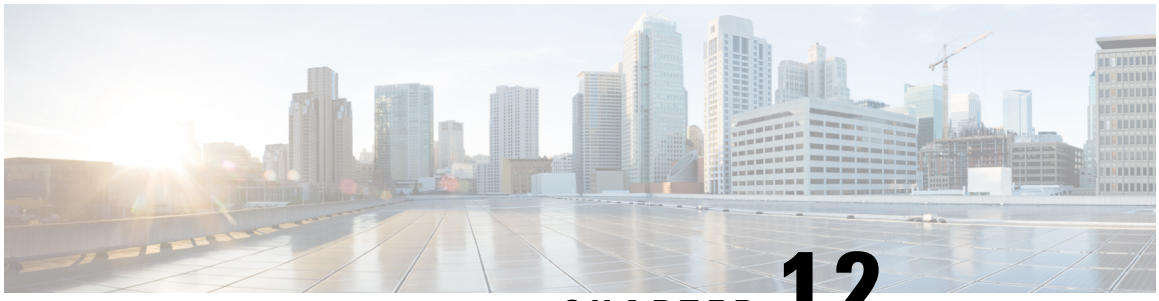
Command Changes

Use the following configuration to enable clearing dynamic route table.

```
configure
  context context_name
    mme-service service_name
      [ no ] clear-route-multipath-zero
  end
```

NOTES:

- **clear-route-multipath-zero**: Enables clearing dynamic route table if diameter lookup finds dynamic route entry with multipath zero. This will take effect only for the subsequent mme diameter session.
- **no**: Disables clearing dynamic route table for multipath zero condition.



CHAPTER 12

Enforcing Detach on Last PDN Deactivation

Feature Summary and Revision History

Summary Data

Applicable Products or Functional Area	MME
Applicable Platforms	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide*

Revision History

Revision Details	Release
MME is enhanced to detach the UE on deletion of the last PDN associated with the NB-IoT. For more information, see the *eDRX Support on the MME* section in the *MME Administration Guide*.	21.27

Feature Description

MME is enhanced to detach the UE on deletion of the last PDN associated with the NB-IoT access type. The enhancement supports a deviation from the 3GPP standards in this respect.

This scenario is applicable only when Attach without PDN Connectivity is enabled for the user.

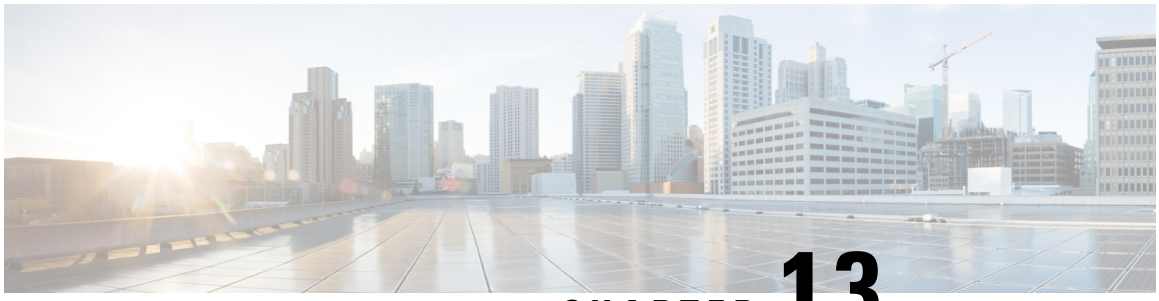
Configuring NB-IoT in UE Context

Use the following configuration to detach the UE on the deletion of the last PDN for NB-IoT access type even if the UE did an attach with Attach Without PDN Connectivity enabled:

```
configure
          call-control-profile profile_name
                    [ remove ] nb-iot ignore-attach-without-pdn
            end
```

NOTES:

- **nb-iot ignore-attach-without-pdn**: Allows detach of Attach-Without-PDN UE after last PDN disconnect.
- **remove**: Disables the existing configuration.



CHAPTER 13

ePDG Support on VPC-DI

Feature Summary and Revision History

Summary Data

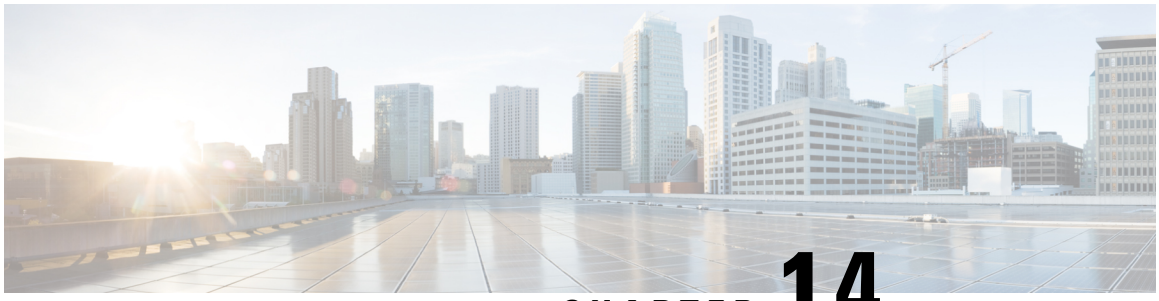
Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable.

Revision History

Revision Details	Release
First introduced.	21.27

Feature Description

ePDG is supported on the VPC-DI platform.



CHAPTER 14

ePDG Interworking with SMF+P-GW-IWK Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - License Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release

ePDG is enhanced to configure ePDG to select P-GW ignoring the SMF based on the selection criteria.	21.27
First introduced.	21.26

Feature Description

Important The 5G interworking feature requires the purchase of an extra license to implement the functionality with the ePDG service.

The ePDG supports a 3GPP feature for 4G (P-GW) vs 5G Session Management Function (SMF) node selection and traffic steering.

To enable 5G mobility from Voice over Wi-Fi (VoWiFi), few parameters get exchanged between UE and SMF (5G) +PGW-IWK. The User Equipment (UE) stores and uses these values during mobility over 5G. The ePDG supports the following functionalities for interworking with SMF+PGW-IWK or P-GW:

1. ePDG selects either SMF+PGW-IWK or P-GW based on three parameters **N1_MODE_CAPABILITY (**UE parameter), **Core-Network-Restrictions** (AAA parameter), and **Interworking-5GS-Indicator** (AAA parameters) AVPs:
   - If the UE supports N1 mode, UE includes the N1_MODE_CAPABILITY Notify payload in the IKE_AUTH Request message.
   - The UE sets the PDU Session ID Value field of the N1_MODE_CAPABILITY Notify payload to a PDU session ID value, which is allocated to the PDU session associated with the IKEv2 security association.
2. ePDG sets 5GSIWK Indication flag to TRUE, in the Create Session Request if:
   - UE is N1 mode capable.
   - Core-Network-Restrictions - 5G core access is not restricted and.
   - Interworking-5GS-Indicator is subscribed
3. If SMF+PGW-IWK is selected and the 5GSIWK flag is TRUE, the ePDG sends PDU Session ID, in the Additional Protocol Configuration Options (APCO) field of Create Session Request, to SMF+PGW-IWK.
4. ePDG sends the 5GCNRS and 5GCNRI indication flags to P-GW or SMF+PGW-C in Create Session Request.
5. SMF+PGW-IWK sends Single – Network Slice Selection Assistance Information (S-NSSAI) to ePDG in the APCO field of Create Session Response.
6. ePDG sends the S-NSSAI to UE in the N1_MODE_INFORMATION Notify payload and PLMN ID in N1_MODE_S_NSSAI_PLMN_ID notify payload of the IKE Auth Response message.

License Requirements

ePDG 5G session count license is required to enable the 5G interworking through the primary CLI, **interworking-5g**, under epdg-service mode. If the CLI is not enabled, all the calls are treated as 4G, ignoring the decision matrix algorithm. For more information on the decision matrix algorithm, refer to the *Selecting P-GW or SMF+PGW-IWK Decision Matrix* section.

Once you update the license, reload the ePDG device for the license to become effective. Without reload, the behavior is undefined.

To configure the license specific CLIs, refer to the *Configuring ePDG to Enable 5G Interworking* and *Configuring ePDG for SMF+PGW-IWK or P-GW*.

Standards Compliance

This feature complies with the following standard procedures for the 5G System (5GS):

3GPP References

- 3GPP TS 24.302: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3”
- 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 23.502: System architecture for the 5G System (5GS)

How it Works

This section provides a call flow and procedure that explains the basic functionality of the ePDG and SMF+P-GW Interworking.

This callflow is followed only when 5G Interworking feature is enabled.

Call Flow

Figure 2: ePDG Setup Procedure Call Flow

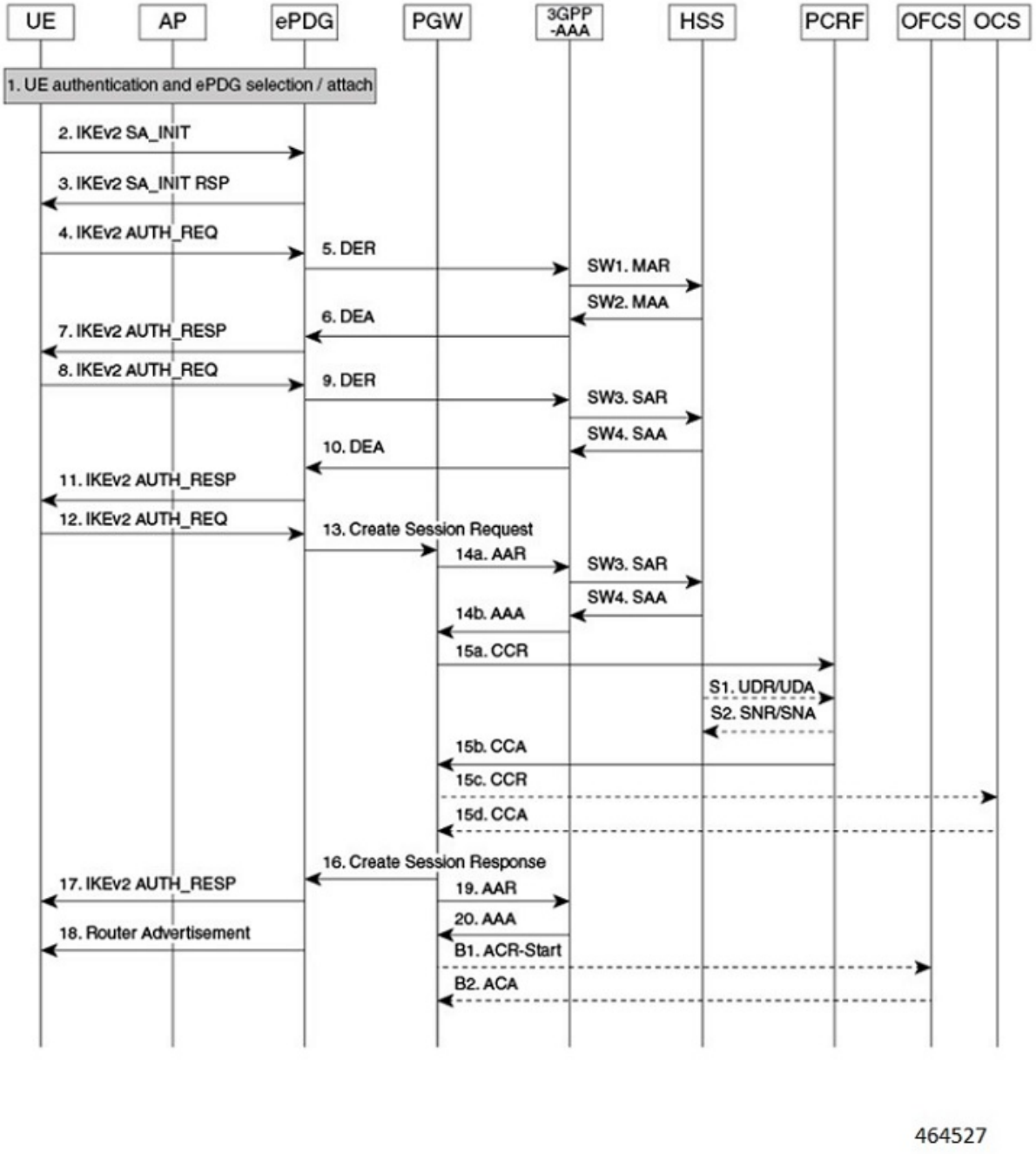


Table 9: ePDG Setup Procedure Call Flow Description

Step	Description
1.	The UE sends the IKE_SA_INIT message.
2.	The ePDG responds with the IKE_SA_INIT_RSP message.
3.	The UE sends the user identity (in the IDI payload) and the APN information (in the IDr payload) in the first message of the IKE_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter to indicate to the ePDG that it wants to use EAP over IKEv2. The user identity is compliant with the Network Access Identifier (NAI) format as specified in *3GPP TS 23.003*. The UE sends the configuration payload (CFG_REQUEST) within the IKE_AUTH request message to obtain an IPv4 home IP Address and/or a Home Agent Address. When the MAC ULI feature is enabled, the root NAI used is of the form "0<IMSI>AP_MAC_ ADDR:nai.epc.mnc<MNC> .mcc<MCC>.3gppnetwork.org". 5GC NAS capable UE indicates its support of 5GC NAS in IKEv2. The UE allocates a PDU Session ID and also includes N1_MODE_CAPABILITY Notify payload.
4.	The ePDG sends the Authentication and Authorization Request message to the 3GPP AAA Server, containing the user identity and APN.
5.	The 3GPP AAA Server fetches the user profile and authentication vectors from HSS/HLR (if these parameters are not available in the 3GPP AAA Server). The 3GPP AAA Server shall look up the IMSI of the authenticated user based on the received user identity (root NAI) and include the EAP-AKA as requested authentication method in the request sent to the HSS. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access. The counter of IKE SAs for that APN is stepped up. If the maximum number of IKE SAs for that APN is exceeded, the 3GPP AAA Server shall send an indication to the ePDG that established the oldest active IKE SA (it could be the same ePDG or a different one) to delete the oldest established IKE SA. The 3GPP AAA Server shall update accordingly the information of IKE SAs active for the APN. The 3GPP AAA Server initiates the authentication challenge. The user identity is not requested again. The AAA server sends the following two parameters if configured: • **Core-Network-Restrictions** • **Interworking-5GS-Indicator** If the AAA server does not send these parameters, ePDG takes default values. For more information on default values, see *Information Element and AVP Support* The ePDG uses these parameters and the 5G NAS capability from the UE to determine if SMF+PGW-IWK or P-GW must be selected.

Step	Description
6.	The ePDG responds with its identity, a certificate, and sends the AUTH parameter to protect the previous message sent to the UE (in the IKE_SA_INIT Exchange). It completes the negotiation of the child security associations if any. The EAP message received from the 3GPP AAA server (EAP-Request/AKA-Challenge) is included to start the EAP procedure over IKEv2.
7.	The UE checks the authentication parameters and responds to the authentication challenge. The only payload (apart from the header) in the IKEv2 message is the EAP message.
8.	The ePDG forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA server.
8a.	The AAA server checks if the authentication response is correct.
9.	When all checks are successful, the 3GPP AAA server sends the final Authentication and Authorization Answer (with a result code indicating success) including the relevant service authorization information, an EAP Success, and the key material to the ePDG. This key material consists of the Primary Session Key (PSK) generated during the authentication process. When the SWm and SWd interfaces between ePDG and 3GPP AAA server are implemented using Diameter, the PSK is encapsulated in the EAP-Primary-Session-Key-AVP, as defined in *RFC 4072*.
10.	The Primary Session Key (PSK) is used by the ePDG to generate the AUTH parameters to authenticate the IKE_SA_INIT phase messages, as specified for IKEv2 in *RFC 4306*. These two first messages were not authenticated before as there was no key material available. According to *RFC 4306 [3]*, the shared secret generated in an EAP Exchange (PSK), when used over IKEv2, is used to generate the AUTH parameters.
11.	The EAP Success or Failure message is forwarded to the UE over IKEv2.
12.	The UE takes its own copy of the PSK as input to generate the AUTH parameter to authenticate the first IKE_SA_INIT message. The AUTH parameter is sent to the ePDG.
12a.	The ePDG checks the correctness of the AUTH received from the UE. At this point, the UE is authenticated.

Step	Description
13.	On successful authentication, the ePDG selects the P-GW or SMF+P-GW-IWK based on Node Selection options. The ePDG sends Create Session Request (IMSI, [MSISDN], Serving Network, RAT Type (WLAN), Indication Flags, Sender F-TEID for C-plane, APN, Selection Mode, PAA, APN-AMBR, Bearer Contexts, [Recovery], [Charging characteristics], [Additional Protocol Configuration Options (APCO)]), Private IE (P-CSCF, AP MAC address). Indication Flags shall have Dual Address Bearer Flag set if PDN Type is IPv4v6. Handover flag is set to Initial or Handover based on the presence of IP addresses in the IPv4/IPv6_Address configuration requests. Selection Mode shall be set to "MS or network provided APN, subscribed verified". The MSISDN, Charging characteristics, APN-AMBR, and bearer QoS shall be provided on S2b interface by ePDG when these are received from AAA on SWm interface. The control plane TEID shall be per PDN connection and the user plane TEID shall be per bearer created. If the UE supports N! mode, is not restricted to interworking with 5GS by user subscription, and access to 5GC is allowed, the ePDG sends the 5GS Interworking Indication flag and PDU Session ID to SMF+PGW-IWK in the Create Session Request. If SMF+PGW-IWK supports more than one S-NSSAI and the APN is valid for more than one S-NSSAI, SMF+PGW-IWK selects one S-NSSAI. **Note** If the UE does not support 5GC NAS but has a 5GS subscription, SMF+PGW-IWK is selected, and if interaction with UDM, Policy Control Function (PCF), and UPF is required, then SMF+PGW-IWK assigns PDU Session ID.
14.	The P-GW allocates the requested IP address to the session and responds back to the ePDG with a Create Session Response (Cause, P-GW S2b Address C-plane, PAA, APN-AMBR, [Recovery], Bearer Contexts Created, [Additional Protocol Configuration Options (APCO)], Private IE (P-CSCF)) message. If SMF+P-GW-IWK receives PDU Session ID, it adds S-NSSAI in the APCO field of Create Session Response.
15.	The ePDG calculates the AUTH parameter which authenticates the second IKE_SA_INIT message.

Step	Description
16.	The ePDG sends the assigned Remote IP address in the configuration payload (CFG_REPLY). The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation stops. The S-NSSAI and the PLMN-ID) is sent to UE, in N1_MODE_INFORMATION Notify and N1_MODE_S_NSSAI_PLMN_ID Notify payload respectively. The N1_MODE_INFORMATION Notify payload indicates to the S-NSSAI for the PDU session associated with the IKEv2 security association established by the IKEv2 message. The PLMN ID corresponding to SNSSAI is sent in N1_MODE_S_NSSAI_PLMN_ID. The N1_MODE_S_NSSAI_PLMN_ID Notify payload indicates to the PLMN ID that the S-NSSAI relates to the PDU session associated with the IKEv2 security association established by the IKEv2 message is carrying the N1_MODE_S_NSSAI_PLMN_ID Notify payload. **Note** If the UE does not support 5GC NAS but has a 5GS subscription, SMF+PGW-IWK is selected, and if interaction with UDM, Policy Control Function (PCF), and UPF is required, then SMF+PGW-IWK assigns PDU Session ID. The SMF+PGW-IWK does not provide any 5GS related parameters to the UE.
17.	Router Advertisement is sent for IPv6 address assignments that is based on configuration. **Note** If the ePDG detects that an old IKE SA for that APN exists, it deletes the IKE SA and sends the UE an INFORMATIONAL Exchange with a Delete payload in order to delete the old IKE SA in UE. If there is any IKEv2 Authentication Response message, the ePDG sends S-NSSAI to the UE.

Information Element and AVP Support

This feature supports the following IE and AVPs:

- PDU Session ID
- S-NSSAI
- Core-Network-Restrictions AVP

  Interworking-5GS-Indicator AVP
- 5GSIWKI (5GS Interworking Indication) Indicator Flag
- 5GCNRS (5GC Not Restricted Support)
- 5GCNRI (5GC Not Restricted Indication)

PDU Session ID

If the UE supports N1 mode, the UE includes the N1_MODE_CAPABILITY Notify payload in the IKE_AUTH Request message. Then, the UE sets the PDU Session ID Value field of the N1_MODE_CAPABILITY Notify payload to a PDU session ID value. The PDU Session ID value is allocated to the PDU session associated with the IKEv2 security association. The ePDG uses N1_MODE_CAPABILITY as one of the parameters to select the P-GW or SMF+PGW-IWK.

S-NSSAI

SMF+PGW-IWK sends the Single – Network Slice Selection Assistance Information (S-NSSAI) to ePDG in the APCO field of Create Session Response. The UE receives this value in N1_MODE_INFORMATION Notify payload.

ePDG sends S-NSSAI to UE in N1_MODE_INFORMATION Notify payload of IKEv2 Authentication Response message.

SMF+PGW-IWK sends S-NSSAI in the APCO field of the Create Session Response message, with Container ID value of 0x001B. This value is parsed, encoded, and sent to UE, in the N1_MODE_INFORMATION Notify payload.

Core-Network-Restrictions

The Core-Network-Restrictions AVP is of type Unsigned32 and contains a bitmask indicating the types of Core Network, which are not allowed for a user.

The following table explains the bits:

Table 10: Meaning of Bits

Bits	Name	Description
0	EPC	Access to EPC not allowed.
1	5GC	Access to 5GC not allowed.
NOTE: Bits not defined in this table will be cleared by the HSS and discarded by the MME.		

Interworking-5GS-Indicator

The Interworking-5GS-Indicator AVP indicates whether the interworking between 5GS and EPS is subscribed or not subscribed for the APN.

The following values are defined in the Interworking-5GS-Indicator AVP:

- NOT-SUBSCRIBED (0)
- SUBSCRIBED (1)

The default value is NOT-SUBSCRIBED (0) when this AVP is not present.

The AAA server sends the Core-Network-Restrictions and Interworking-5GS-Indicator AVPs in the DEA (Diameter EAP Answer) Response message.

5GSIWKI Indicator Flag

The 5GSIWKI flag is set to 1 for UEs supporting N1 mode and not restricted from interworking with 5GS by user subscription and access to 5GS is allowed for the PDN connection.

The 5GSIWKI Indicator flag is sent to SMF+PGW-IWK in the Create Session Request message.

5GCNRS Flag

When 5GCNRS bit is set to 1, it indicates to the PGW-C+SMF+PGW-IWK that the MME or ePDG node supports 5GCNRI flag settings.

Note This flag is always set to 1 from the 3GPP TS29.274 Rel 16 support.

5GCNRI Flag

When the 5GCNRI flag is set to 1, it indicates to the PGW-C+SMF+PGW-IWK that access to the 5GC is open for the PDN connection without any restriction.

However, when the 5GCNRS flag is set to 1 and the 5GCNRI flag is set to 0, access to the 5GC is restricted for the PDN connection. PGW-C+SMF+PGW-IWK does not consider the 5GCNRI flag if the 5GSIWKI flag is set to 1. It happens when the 5GS Interworking is supported for PDN connection.

Note This flag is set to 1, when the **Core-Network-Restrictions** is allowed for 5G and Interworking-5GS-Indicator is Subscribed.

Selecting P-GW or SMF+PGW-IWK Decision Matrix

The ePDG uses the following decision matrix for selecting the SMF+PGW-IWK or P-GW, to establish the PDN connectivity.

If the ePDG 5G license is not present or **`interworking-5g`** under epdg-service is not enabled, the ePDG ignores the following decision matrix algorithm. All calls are treated as 4G calls regardless of any parameter mentioned in the following table.

Figure 3: P-GW or SMF+PGW-IWK Decision Matrix Table

Scenario	UE 5GC NAS Capability	Core-Network-Restrictions	Interworking-5GS APN-Configuration	MME Policy	Service Tag for Selection of DNS Records by MME (NOTE 0)	5GSIWKI	5GCNRS	5GCNRI	P-GW or SMF
							Rel-15: Not Applicable Rel-16: Values below		
	From UE	From HSS				+On S11+S5/ S2b			
1-2	Yes or No	Not Included	Not Included	No	x-s2bc-gtp	0	1	0	P-GW
3	No	Not Included	SUBSCRIBED	Operator Policy (NOTE1)	x-s2bc-gtp+nc-smf (default) x-s2bc-gtp	0	1	1	SMF (Default) P-GW
4	Yes	Not Included	SUBSCRIBED	No	x-s2bc-gtp+nc-smf	1	1	1	SMF
5	No	Not Included	NOT SUBSCRIBED	Operator Policy (NOTE 1) (NOTE 2)	x-s2bc-gtp+nc-smf (default) x-s2bc-gtp	0	1	0	SMF (Default) P-GW
6	Yes	Not Included	NOT SUBSCRIBED	Operator Policy (NOTE 2)	x-s2bc-gtp+nc-smf (default) x-s2bc-gtp	0	1	0	SMF (Default) P-GW
7-12	Yes or No	5GC Not Allowed	SUBSCRIBED or Not SUBSCRIBED or Not Included	No	x-s2bc-gtp	0	1	0	P-GW
13	No	5GC Allowed	SUBSCRIBED	Operator Policy (NOTE1)	x-s2bc-gtp+nc-smf (default) x-s2bc-gtp	0	1	1	SMF (Default) P-GW
14	Yes	5GC Allowed	SUBSCRIBED	No	x-s2bc-gtp+nc-smf	1	1	1	SMF
15-16	No	5GC Allowed	NOT SUBSCRIBED or Not Included	Operator Policy (NOTE 1) (NOTE 2)	x-s2bc-gtp+nc-smf (default) x-s2bc-gtp	0	1	0	SMF (Default) PGW
17-18	Yes	5GC Allowed	NOT SUBSCRIBED or Not Included	Operator Policy (NOTE 2)	x-s2bc-gtp+nc-smf (default) x-s2bc-gtp	0	1	0	SMF (Default) P--GW

464608

NOTE 0: For P-GW, replace "-s2bc" by "-s2b", so that "x-s2bc-gtp" becomes "x-s2b-gtp".

NOTE 1:

- Default Behavior: SMF+PGW-IWK supports Rel-16 functionality to support 4G-only UEs, that is, the SMF+P-GW-IWK is able to generate PDU Session ID for 4G-only UEs.
- Custom Behavior: To handle the case where SMF+P-GW-IWK is Rel-15 and cannot support 4G only UEs.

NOTE 2:

- Default Behavior: When Interworking-5GS APN-Configuration is set to disallow the APN configuration in UDR, but handover to 5G SA is not allowed.
- Custom Behavior: When Interworking-5GS APN-Configuration is set to disallow the APN configuration in SPR and not in UDR, then P-GW is selected.

NOTE 3:

The **pgw smf-not-configured** CLI allows you to configure whenever the SMF IPs are not updated in DNS or local ePDG configuration, so that ePDG ignores the SMF selection and always selects the P-GW based on selection criteria.

In the P-GW or SMF+PGW-IWK Decision Matrix table:

1. For scenarios 1 and 2, the operator has not updated the subscription. Hence, HSS doesn’t include the 'Core-Network-Restrictions' flag or 'Interworking-5GS-Indicator' in the subscription. In such scenarios, the operator selects the P-GW. However, in scenarios 3-18, the existing 4G subscriptions are modified. The operator selects either the 5GC restriction flag or the 5G interworking indication flag in the subscription.
2. For scenarios 3 and 13, the operator has subscribed to the interworking with 5GS. Since the UE is 4G-only, the operator may select SMF+PGW-IWK.
3. In scenarios 5-6 and 15-18, 5GC is allowed. However, the interworking with 5GS is not supported for the PDN connection. Ideally, the operator may select SMF+PGW-IWK for these scenarios since a 5G subscription exists. However, some operators can also anchor the PDN connection on P-GW.
4. In scenarios 7-12, the subscriber must not use the 5GC. Hence, the operator should not select SMF+PGW-IWK irrespective of the values of other parameters.
5. In scenarios 4 and 14, the UE supports 5G. The 5GC is allowed. The PDN connection is handed over to 5G Stand Alone (SA). Hence, the operator can select SMF+PGW-IWK.

From the previous matrix, if SMF+PGW-IWK is selected, the e-PDG uses the S-NAPTR procedure with the service parameters of *x-s2b-gtp+nc-smf* in the following scenarios:

- AAA provided FQDN-based P-GW selection
- APN-FQDN based P-GW selection
- Local FQDN-based P-GW selection

Fallback Mechanism for Selecting Combined SMF+PGW-IWK

The following table describes the fallback mechanism for selecting combined SMF+PGW-IWK or P-GW.

Table 11: Fallback Mechanism

SMF+PGW-IWK or P-GW	Service Parameter	Selection Order
SMF+PGW-IWK	**x-s2b-gtp+nc-smf**	If ePDG selects SMF from the decision matrix, using the x-s2b-gtp+nc-smf service parameter, the following are the possible scenarios from the DNS server: **1.** If DNS response has records for SMFs and if the selected SMFs are not reachable, the fallback to static SMF selection works based on the local configuration. **2.** If DNS response has no SMF records but has P-GW records, then ePDG ignores the P-GW list and fallback to static SMF selection. **3.** If the DNS query fails, there are no SMF records, or DNS is not reachable then, ePDG fallback to static SMF selection based on the local configuration. The appropriate DNS-related failures get incremented. In case of Local Static selection: • If SMFs are configured, that will be considered: • If weight is defined, then, the Weight algorithm similar to the existing P-GW selection is applied to SMF+P-GW-IWK. • If no weight is configured, SMF+PGW-IWK is selected in a round robin manner. • If no SMF+PGW-IWK is configured and only has P-GW, then ePDG ignores the P-GW lists and SMF+PGW-IWK selection fails, a call gets terminated with appropriate disconnect reasons. If initial selection preference is local static, instead of DNS, then same fallback mechanism is followed vice-versa with local SMF->DNS SMF selection. The fallback mechanism, priority, and preference order of selection based on various criteria between AAA provided IP, DNS, and Static remains the same as legacy P-GW selection, and applicable to SMF+PGW-IWK.

SMF+PGW-IWK or P-GW	Service Parameter	Selection Order
P-GW	**x-s2b-gtp**	If ePDG selects only P-GW, the output is generated from the DNS response using the x-s2b-gtp service parameter. The following are the possible scenarios from the DNS server: **1.** If DNS response has records for P-GW and if the selected P-GW are not reachable, Fallback to static P-GW selection occurs based on local configuration. **2.** If DNS response has no P-GW records but has SMF records, then ePDG ignores the SMF and fallback to static P-GW selection. **3.** If DNS query fails or no P-GW records are found, or DNS is not reachable, then fallback to static P-GW selection occurs based on the local configuration. In case of Local Static selection: • If P-GWs are configured, it will be considered. • If weight is defined, then, the Weight algorithm similar to the existing P-GW selection is applied. • If no weight is configured, P-GW is selected in a round robin manner. • If no P-GW is configured and only has SMF, then ePDG ignores the SMF lists and SMF+PGW-IWK selection fails, a call gets terminated with appropriate disconnect reasons. If no local static entries are defined for P-GW: P-GW selection fails and the call gets terminated with the appropriate disconnect reasons. If initial selection preference is local static instead of DNS, then, ePDG performs a fallback and the opposite way with the local SMF->DNS SMF selection.

In handover scenarios, ePDG considers the AAA provided P-GW-ID (IP address or FQDN) for P-GW or SMF+PGW-IWK selection.

Limitations

This feature has the following limitations:

- The ePDG support is applicable only for the 4G or 5G NAS capable devices attached to ePDG through the legacy 4G message. ePDG does not support 5G NAS request directly sent to ePDG.

- SMF+PGW-IWK support is limited to the GTPv2 based S2b interface.
- The emergency attach flow is not supported because for 5G NAS capable devices, the emergency VoWIFI call is not supported through ePDG.

Configuring ePDG to Enable 5G Interworking

The 5G Interworking feature is enabled only if the ePDG 5G license is configured. If the ePDG license is not present or the 5G interworking feature is not enabled, by default the ePDG selects the P-GW as per the legacy behavior.

When the interworking feature is enabled, Capability of UE, AAA 5G attributes, and other 5G custom behavior CLIs influence the P-GW or SMF+PGW-IWK selection. 5G Interworking CLIs to customize P-GW or SMF+PGW-IWK selection are available only when 5G interworking feature is enabled.

Use the following configuration to enable or disable the 5G interworking on ePDG:

```
configure
    context context_name
      epdg-service service_name
         [ no ]  interworking-5g
         end
```

NOTES:

- **interworking-5g**: Enables the 5G interworking for the ePDG service.
- **[no] interworking-5g**: If disabled, all calls are treated as 4G.

Configuring ePDG for SMF+PGW-IWK or P-GW

The ePDG selects SMF+PGW-IWK as per the default behavior. This default behavior is customized using the configuration command under ePDG-service mode to choose P-GW.

Configuring ePDG to Select P-GW for 4G-Only UE

For 4G-only UEs, operator network configuration can latch on SMF+PGW-IWK. If operator does not have support for SMF+PGW-IWK, the operator has the choice to configure to select P-GW for 4G-only UEs.

Use the following configuration to enable or disable P-GW selection for 4G-only UE:

```
configure
    context context_name
      epdg-service service_name
         [ no ] pgw-selection select pgw 4gonly-ue
         end
```

NOTES:

- **pgw-selection select pgw 4gonly-ue**: If enabled for 4G only UE, ePDG selects the P-GW by overriding the default SMF selection.
- **no pgw-selectionselect pgw 4gonly-ue**: If disabled for 4G only UE, then P-GW selection is reverted to default selection of SMF+P-GW-IWK.

This command is configurable only when interworking-5g is enabled.

Configuring ePDG to Consider Interworking-5GS-Indicator

As per the default behavior, the ePDG may select SMF+PGW-IWK, if the 5GS interworking is not subscribed. If the operator network configuration does not support SMF+PGW-IWK, use the following configuration to override this default behavior and select P-GW as a preferred node:

```
configure
    context context_name
      epdg-service service_name
         [ no ] pgw-selection select pgw  no-5gs-interworking
         end
```

NOTES:

- **pgw-selection select pgw no-5gs-interworking** : If enabled for 5Gs interworking not subscribed cases, P-GW will be selected by overriding the default SMF+PGW-IWK selection.
- **no pgw-selection select pgw no-5gs-interworking** : If disabled, P-GW selection gets reverted to default selection of SMF+P-GW-IWK for 5GS interworking not subscribed cases.

This command is configurable only when interworking-5g is enabled.

Configuring ePDG to Select P-GW to Ignore the SMF Selection

When an operator has not updated the SMF IP or fully qualified domain name (FQDN) in DNS server or in local ePDG configuration, use the following command to ignore SMF+PG-IWK selection and always select P-GW:

Enabling the **pgw smf-not-configured** option overrides the **4gonly-ue** and **no-5gs-interworking** options.

```
configure
    context context_name
      epdg-service  service_name
          [ no ] pgw-selection select pgw smf-not-configured
          end
```

NOTES:

- **pgw-selectionselect pgw smf-not-configured**: Once enabled, ePDG ignores the SMF selection and always choose P-GW by overriding **4gonly-ue** and **no-5gs-interworking** options.
- **no**: Disables pgw-selection related parameters for the ePDG service.

This command is configurable only when interworking-5g is enabled.

Configuring ePDG in the Local SMF+PGW-IWK Node

Use the following configuration command to configure SMF+PGW-IWK:

```
configure
    apn-profile apn_name
      pgw-address ip_address smf-combined
      end
```

NOTES:

- **pgw-address** *ip_address* **smf-combined**: Configures SMF+PGW-IWK for the specified IPv4 or IPv6 address.

Configuring ePDG 5G Interworking Bulk Statistics

Use the following configuration to configure the **epdg-interworking-5g** bulkstats schema. This configuration is only available upon license and 5G interworking is enabled.

```
configure
    bulkstat mode
        [ no ] epdg-interworking-5g schema schema_name
       end
```

NOTES:

- **epdg-interworking-5g schema** *schema_name* **format**: Allows ePDG to capture 5G interworking related bulk statistics.

Monitoring and Troubleshooting

This section provides information to monitor and troubleshoot this feature using show commands.

Show Commands and Outputs

This section provides information about the show commands and outputs for the ePDG 5G interworking feature.

show epdg-service statistics interworking-5g

The **show epdg-service statistics interworking-5g** command displays output of Interworking 5G statistics at system-level. The **show epdg-service name** *epdg-service-name* **statistics interworking-5g** command displays output of Interworking 5G statistics for a particular ePDG-service. The **interworking-5g** option is available only with ePDG 5G license.

Table 12: show epdg-service statistics interworking-5g Command Output Descriptions

Field	Description
5G Sessions – Counter for sessions from N1 mode capable UEs	

Field	Description
Attempts	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE.
Setup	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE and that call succeeds.
Failures	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE and that call fails due to some failure reason.
P-GW/SMF selection type – Based on the 5G capability flags and related CLI, the PDN request is forwarded to P-GW or SMF+PGW-IWK	
SMF preferred	The number of times that SMF is chosen for this call, but IWK flag is not set.
SMF only	The number of times that ePDG selects SMF for this call, IWK flag is set, and PDU Session ID is forwarded to SMF.
DNS provided SMF	The number of times that SMF is selected from DNS responses.
Locally configured SMF	The number of times that SMF is selected from the local ePDG configuration.
AAA provided SMF IP	The number of times that ePDG selects SMF from the AAA server provided IP attribute.
P-GW only	The number of times P-GW is selected.
DNS provided P-GW	The number of times that P-GW is selected from DNS responses.
Locally configured P-GW	The number of times that P-GW is selected from the local ePDG configuration.
AAA provided P-GW IP	The number of times that P-GW is selected from the AAA server provided IP attribute.
P-GW or SMF not available reasons - Provide counters on how many times the SMF or P-GW selection is failed due to P-GW or SMF is not locally configured.	
No P-GW configured locally	The number of times that P-GW selection failed due to missing configuration.
No SMF configured locally	The number of times that SMF+PGW-IWK selection failed due to missing configuration.
SMF Fallback Support Statistics for GTP nodes – Fallback-related counters for SMF provided by AAA, DNS, and local configuration. In general, an attempt for second SMF or P-GW after the first SMF or P-GW is failed is considered as fallback.	

Field	Description
SMF Fallback Attempted	The number of times that fallback is attempted when SMF is preferred. Increments after it fails to connect to the first SMF and attempts the second SMF. This includes SMFs provided by AAA, DNS, and the local configuration.
SMF Fallback Success	The number of times that a session connected to SMF is selected through the fallback algorithm.
SMF Fallback Failure	The number of times that a session, which is unable to connect to SMF is selected through a fallback algorithm.
Alternate SMF not found	The number of failed attempts to SMF and there is no alternate SMF available to attempt and connect to a session.
Local SMF resolution	Fallback related counters for SMF by local configuration. These counters are not incremented if the first SMF is selected from the local configuration despite trying to connect to the DNS/AAA provided SMF.
SMF Fallback Attempted	The number of times that fallback is attempted when SMF is preferred. Increments after it fails to connect to the first SMF and attempts the second SMF. This includes SMFs provided by AAA, DNS, and local configuration.
SMF Fallback Success	The number of times that a session connected to SMF is selected through the fallback algorithm.
SMF Fallback Failure	The number of times that a session, which is unable to connect to SMF is selected through the fallback algorithm.
Alternate SMF not found	The number of times that attempts to SMF fail and there is no alternate SMF available for a session to connect.
P-GW Fallback Support Stats for GTP nodes - Fallback related counters for P-GW provided by AAA, DNS, and local configuration. In general, an attempt considers as fallback, after failed to connect to the first SMF/P-GW.	
P-GW Fallback Attempted	The number of times that fallback is attempted when P-GW is preferred. Increments after it fails to connect to the first P-GW and attempts for the second P-GW. This includes P-GW provided by AAA, DNS, and local configuration.
P-GW Fallback Success	The number of times that a session connected to P-GW is selected through the fallback algorithm.
P-GW Fallback Failure	The number of times that a session, which is unable to connect to P-GW is selected through the fallback algorithm.
Alternate P-GW not found	The number of failed attempts to all P-GW, and there is no alternate P-GW available to attempt for a session to connect.

Field	Description
Local P-GW resolution	Fallback related counters for P-GW provided by local configuration. These counters do not get incremented if the first SMF selected from the local configuration gets connected, even after attempting the DNS/AAA provided SMF.
P-GW Fallback Attempted	The number of times that fallback is attempted when P-GW is preferred. Increments after it fails to connect to the first P-GW and attempts for the second P-GW. This includes P-GW provided by AAA, DNS, and local configuration.
P-GW Fallback Success	The number of times that a session connected to P-GW is selected through the fallback algorithm.
P-GW Fallback Failure	The number of times that a session fails to connect to P-GW and selected through the fallback algorithm.
Alternate P-GW not found	The number of failed attempts to all P-GW, and there is no alternate P-GW available to attempt for a session to connect.
DNS-related Failures	
DNS server not reachable	The number of times when no response from DNS.
No resource records	The number of times that the DNS server responded with no resource records.
No matching P-GW service params	The number of times that the DNS server responded with no P-GW in the resource records, when P-GW is the preferred gateway for the session.
No matching SMF service params	The number of times that the DNS server responded with no SMFs in the resource records, when SMF is the preferred gateway for the session.
DNS P-GW list exhausted	The number of failed attempts to connect to all the P-GW provided by DNS response, when P-GW is the preferred gateway for the session.
DNS SMF list exhausted	The number of failed attempts to connect to all the SMF provided by DNS response, when SMF is the preferred gateway for the session.

show configuration

If the following commands are configured, the output of this CLI command displays the following parameters under ePDG-service:

- Service name:
  - **interworking-5g**: Displays the enabled 5G interworking for the ePDG service.
  - **pgw-selection select pgw 4g-only-ue**: Displays the enabled P-GW for 4G-only-UE.

- **pgw-selection select pgw no-5gs-interworking**: Displays the enabled P-GW selection for 5Gs interworking.
- **pgw-selection select pgw smf-not-configured**: Displays the enabled P-GW selection. ePDG ignores SMF, even if the SMF IP/FQDN is configured in DNS/local ePDG config.

The following is a sample output:

```
config
cli hidden
tech-support test-commands encrypted password ***
....
.....
epdg-service epdg1
plmn id mcc 242 mnc 002
associate egtp-service egtp-epdg-egress-v4
ebi range start 10 end 13
pgw-selection agent-info error-terminate
dns-pgw selection topology weight
associate qci-qos-mapping epdg_mapping
associate subscriber-map map1
associate lte-emergency-profile emergency
username check-mac-address failure-handling continue
reporting-action event-record
max-sessions 100000
bind address 111.111.11.2 crypto-template boston
interworking-5g
pgw-selection select pgw 4gonly-ue
pgw-selection select pgw no-5gs-interworking
pgw-selection select pgw smf-not-configured
#exit
```

show epdg-service name

If the following commands are configured, the output of **show epdg-service name** *service name* CLI command displays the following parameters under ePDG-service:

- Service name:
  - **interworking-5g**: Displays enabled 5G interworking for the ePDG service.
  - **pgw-selection select pgw**: Displays the enabled P-GW for 4G-only-UE and 5GS indicator.
  - **pgw-selection select pgw no-5gs-interworking**: Displays the enabled P-GW selection for 5Gs interworking.
  - **pgw-selection select pgw smf-not-configured**: Displays the enabled P-GW selection. ePDG ignores SMF, even if the SMF IP/FQDN is configured in DNS/local ePDG config.

The following is a sample output:

```
Service name: epdg1
Context: pdif
Bind: Done
Max Sessions : 100000
IP address: 111.111.11.2 UDP Port : 500
Crypto-template: boston
Reporting Action:
Event Record: Enabled
Service State: Started Service Id: 6
EGTP service : egtp-epdg-egress-v4
```

```
MAG service : n/a
MAG context : n/a
PLMN Id: MCC:242 , MNC:002
Setup Timeout (sec) : 60
dns-pgw context: pdif
dns-pgw selection : weight,topology
fqdn: n/a
pgw-selection agent-info error-handling: terminate
pgw-selection select PGW: 4G Only UE, No 5GS Interworking, SMF Not Configured
Custom SWm-SWu Error Mapping: Disabled
Custom S2b-SWu Error Mapping: Disabled
3GPP SWu Private Notify Error Types: Disabled
Preferred PGW selection mechanism: AAA/DNS
vendor-specific-attr dns-server-req: APCO
vendor-specific-attr pcscf-server-req: Private Extension
Username MAC Address Stripping : Disabled
QCI QOS Mapping Table : epdg_mapping
Username MAC Address Validate : Enabled Failure-handling : Continue
Newcall Policy : None
Duplicate precedence in TFT - Allowed
IP Fragment-Chain Timeout : 5 sec and Max OOO Fragment : 45
EBI :
Allowed Range 10 to 13
Username MAC Address Delimiter - colon-or-NAI-Label
Subscriber Map : map1
AAA Send Framed-MTU Size : Disabled
Data Buffering : Enabled
PDN-type IPv6 Path-MTU : Enabled
GTPC Overload Control Profile : None
GTPC Load Control Profile: None
LTE Emergency Profile: emergency
Timeout Idle : Disabled
Suppress International Roamer Handover : Disabled
5G Interworking : Enabled
```

Bulk Statistics

This section provides information on the bulk statistics variables for the **epdg-interworking-5g** schema. This schema is available upon installing 5G license.

show bulkstats variables epdg-interworking-5g

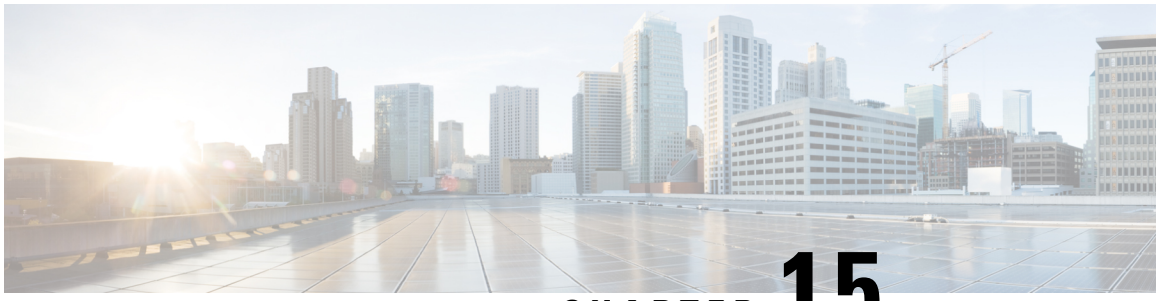
Use this command to display the list of bulk statistics variables supported by **epdg-interworking-5g schema**.

Bulk Statistics Variables	Description
5G Sessions:	
iwk5g-5gsessions-attempted	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE.
iwk5g-5gsessions-setup	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE and that call succeeds.
iwk5g-5gsessions-failure	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE and that call fails due to some failure reason.

P-GW/SMF selection type:	
iwk5g-smf-preferred	The number of times that SMF is selected as the first preference. Increments when SMF is chosen for this call, but the IWK flag is not set.
iwk5g-smf-preferred-dns	The number of times that SMF is selected from DNS responses.
iwk5g-smf-preferred-local	The number of times that SMF is selected in the local ePDG configuration.
iwk5g-smf-preferred-aaa	The number of times that ePDG selects the SMF in the AAA server provided IP attribute.
iwk5g-smf-only	The number of times when ePDG selects SMF for this call, IWK flag is set, and PDU Session ID is forwarded to SMF.
iwk5g-smf-only-dns	The number of times that SMF is selected from DNS responses.
iwk5g-smf-only-local	The number of times that SMF is selected in the local ePDG configuration.
iwk5g-smf-only-aaa	The number of times that ePDG selects the SMF from the AAA server provided IP attribute.
iwk5g-pgw-only	The number of times that P-GW is selected.
iwk5g-pgw-only-dns	The number of times that P-GW is selected from DNS responses.
iwk5g-pgw-only-local	The number of times that P-GW is selected in the local ePDG configuration.
iwk5g-pgw-only-aaa	The number of times that P-GW is selected in the AAA server provided IP attribute.
iwk5g-no-local-pgw	The number of times that P-GW is unable to select due to missing local configuration.
iwk5g-no-local-smf	The number of times that P-GW is unable to select SMF+PGW-IWK due to missing configuration.
SMF Fallback Support Stats for GTP nodes:	
iwk5g-smf-fallback-attempted	The number of times that fallback is attempted when SMF is preferred. Increments after it fails to connect to the first SMF and attempts the second SMF. This includes SMFs provided by AAA, DNS, and local configuration.
iwk5g-smf-fallback-success	The number of times that a session connected to SMF is selected through the fallback algorithm.

iwk5g-smf-fallback-failed	The number of times that a session unable to connect to SMF is selected through the fallback algorithm.
iwk5g-smf-fallback-noalt-smf	The number of failed attempts to all SMF, and there is no alternate SMF available to attempt and connect to a session
Local SMF resolution:	
iwk5g-local-smf-fallback-attempted	The number of times that fallback is attempted when SMF is preferred. Increments after it fails to connect to the first SMF and attempts the second SMF. This includes SMFs provided by AAA, DNS, and local configuration.
iwk5g-local-smf-fallback-success	The number of times that a session connected to SMF is selected through the fallback algorithm.
iwk5g-local-smf-fallback-failed	The number of times that a session unable to connect to SMF is selected through the fallback algorithm.
iwk5g-local-smf-fallback-noalt-smf	The number of failed attempts to all SMF, and there is no alternate SMF available to attempt and connect to a session.
P-GW Fallback Support Stats for GTP nodes:	
iwk5g-pgw-fallback-attempted	The number of times that fallback is attempted when P-GW is preferred. Increments after it fails to connect to the first P-GW and attempts for the second P-GW. This includes P-GW provided by AAA, DNS, and local configuration.
iwk5g-pgw-fallback-success	The number of times that a session connected to P-GW is selected through the fallback algorithm.
iwk5g-pgw-fallback-failed	The number of times that a session unable to connect to P-GW is selected through the fallback algorithm.
iwk5g-pgw-fallback-noalt-pgw	The number of failed attempts all P-GW, and there is no alternate P-GW available to attempt and connect to a session.
Local P-GW resolution:	
iwk5g-local-pgw-fallback-attempted	The number of times that fallback is attempted when P-GW is preferred. Increments after it fails to connect to the first P-GW and attempts for the second P-GW. This includes P-GW provided by AAA, DNS, and local configuration.
iwk5g-local-pgw-fallback-success	The number of times that a session connected to P-GW is selected through the fallback algorithm.

iwk5g-local-pgw-fallback-failed	The number of times that a session fails to connect to P-GW is selected through the fallback algorithm.
iwk5g-local-pgw-fallback-noalt-pgw	The number failed attempts to all P-GW, and there is no alternate P-GW available to attempt and connect to a session.
DNS-related Failures:	
iwk5g-dns-server-notreachable	The number of times that there is no response from DNS.
iwk5g-dns-no-resourcerecords	The number of times that the DNS server responded with no resource records.
iwk5g-dns-no-matching-pgw-service	The number of times that the DNS server responded with no P-GW in the resource records, when P-GW is the preferred gateway for the session.
iwk5g-dns-no-matching-smf-service	The number of times that the DNS server responded with no SMFs in the resource records, when SMF is the preferred gateway for the session.
iwk5g-dns-pgw-list-exhausted	The number of times that P-GW provided by DNS response failed to connect, when P-GW is the preferred gateway for the session.
iwk5g-dns-smf-list-exhausted	The number of times that SMF provided by DNS response failed to connect, when SMF is the preferred gateway for the session.



CHAPTER 15

IKEv2 Authentication Failure Counters

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Statistics and Counters Reference - Bulkstatistic Descriptions* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.27

Feature Description

ePDG supports IKEv2 authentication failure counters for Voice over Wi-Fi sessions.

These counters can segregate IKEv2 authentication failure and can be used to identify and exclude failure scenarios from the IKEv2 Authentication Success Rate calculation criteria.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available in support of this feature.

Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show crypto statistics ikev2

The output of this command is enhanced to display the following fields.

Table 13: show crypto statistics IKEv2 Command Output Descriptions

Field	Description
IKEv2 Authentication Failures	
No DEA message	The total number of non DEA messages.
Missing AVP in DEA	The total number of missing AVPs in the DEA message.
Invalid APN	The total number of invalid APNs.
Key mismatch	The total number of key mismatches in the authentication vectors.
Invalid result code or AVP in DEA	The total number of invalid result code or AVP in the DEA message.
Invalid NAI format	The total number of invalid NAI formats.
APN validation failed	The total number of failed APN validations.
Misc. auth failures	The total number of miscellaneous authentication failures.

Similarly, you can view the IKEv2 authentication failure counters using the **show crypto statistics ikev2 service-name** command.

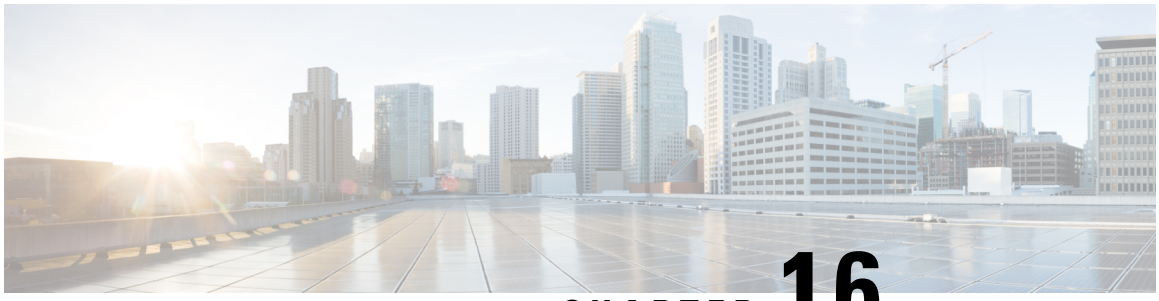
Bulk Statistics

The ePDG schema supports the following bulk statistics:

ePDG Schema

Table 14: Bulk Statistics Variables in the ePDG Schema

Variables	Description
ikev2-auth-failnodea	The total number of non DEA messages.
ikev2-auth-failinvresoravp	The total number of invalid result code or AVP in the DEA message.
ikev2-auth-failmissingavp	The total number of missing AVPs in the DEA message.
ikev2-auth-failinvnaiformat	The total number of invalid NAI formats.
ikev2-auth-failinvapn	The total number of invalid APNs.
ikev2-auth-failapnvalfailed	The total number of failed APN validations.
ikev2-auth-failkeymismatch	The total number of key mismatches in the authentication vectors.
ikev2-auth-failmiscauth	The total number of miscellaneous authentication failures.



CHAPTER 16

LTE-M RAT Indication Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.27

Feature Description

MME parses and stores the LTE-M RAT Indication IE in UE Capability Info Indication message. For Category M UEs, MME sends the RAT type of LTE-M (9) in the RAT type IE to S-GW. MME requests S-GW to pass the LTE-M RAT type to P-GW. The request to P-GW is based on the LTE-M RAT type indication configuration under call-control profile and mme-service. Based on the configuration, the LTEMPI (LTE-M RAT type reporting to P-GW Indication) bit in Indication IE is set in the create session request and modify bearer request messages to S-GW. The LTEMPI bit set to 1 indicates that the S-GW forwards the LTE-M RAT type to P-GW.

The Inter-MME changes the source and sends the LTE-M indication to the target MME. The source MME sends the indication message through the LTEMUI (LTE M UE Indication) bit in forward relocation request message and context response message over S10. The LTEMUI is set to 1 for Category M UEs. For other RAT types, the value is set to 0.

Configuration Support for LTE-M RAT Type Reporting to P-GW

Configuring LTEMPI Flag under Call Control Profile

Use the following configuration commands to configure the LTEMPI flag under call control profile:

```
configure
  call-control-profile profile_name
    lte-m-rat flag-LTEMPI { 1 | 0 }
      [ no | default | remove ] lte-m-rat
      end
```

NOTES:

- **lte-m-rat**: Enables configuration for LTE-M Access type.
- **flag-LTEMPI**: Configures LTE-M RAT Indication to S-GW to pass the LTE-M RAT type to the P-GW.
- **[no | default | remove]**: Removes the configuration from call-control profile and fallback to the mme-service configuration.

Configuring LTEMPI Flag under MME Profile

Use the following configuration commands to configure the LTEMPI flag under MME profile:

```
configure
  context context_name
    mme-service service_name
      lte-m-rat flag-LTEMPI { 0 | 1 }
        [ no | default ] lte-m-rat
        end
```

NOTES:

- **lte-m-rat**: Enables configuration for LTE-M Access type.
- **flag-LTEMPI**: Configures LTE-M RAT Indication to S-GW to pass the LTE-M RAT type to the P-GW.
- **[no | default | remove]**: Removes the configuration from call-control profile and fallback to the mme-service configuration.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available in support of this feature.

Show Command and Output

This section provides information about the show commands and outputs in support of this feature.

show mme-service { all | name <service name> }

The output of this command displays the following field:

Field	Description
LTE-M RAT Indication to S-GW to pass the LTE-M RAT type to the P-GW (Enabled/Disabled)	Displays the enabled or disabled status of the LTE-M RAT Indication to P-GW.

show call-control-profile full { all | name <ccp name> }

The output of this command displays the following field:

Field	Description
LTE-M RAT Indication to S-GW to pass the LTE-M RAT type to the P-GW (Enabled/Disabled)	Displays the enabled or disabled status of the LTE-M RAT Indication to P-GW.

show subscribers mme-only { all | full all | wf1 all } imsi <imsi_name>

The output of this command displays the following field:

Field	Description
Access Tech : (R) - LTE-M	Displays the Access Tech as 'R' (LTE-M) for Category M UEs.

show subscribers mme-service <service_name> imsi

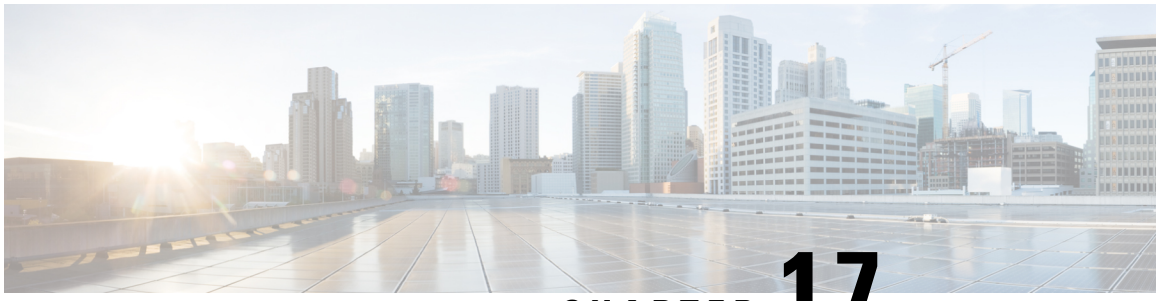
The output of this command displays the following field:

Field	Description
Access Tech : (R) - LTE-M	Displays the Access Tech as 'R' (LTE-M) for Category M UEs.

Bulk Statistics

This section provides information on the bulk statistics variables for the MME schema:

Bulk Statistics Variables	Description
LTE-M Attached Calls	Displays the current total number of attached low power Subscribers operating in Category M.



CHAPTER 17

No IMSI or MSISDN Included in LRR for VoLTE EM Call from User of Foreign Network

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide*

Revision History

Revision Details	Release
Unauthorized IMSI is sent in the LRR message using the CLI.	• 21.27 • 21.26 • 21.25.6

Feature Changes

Previous Behavior: Unauthorized International Mobile Subscriber Identity (IMSI) is not sent in the LRR message.

New Behavior: The **unauth-imsi** CLI allows MME to send unauthorized IMSI in the LRR message when available.

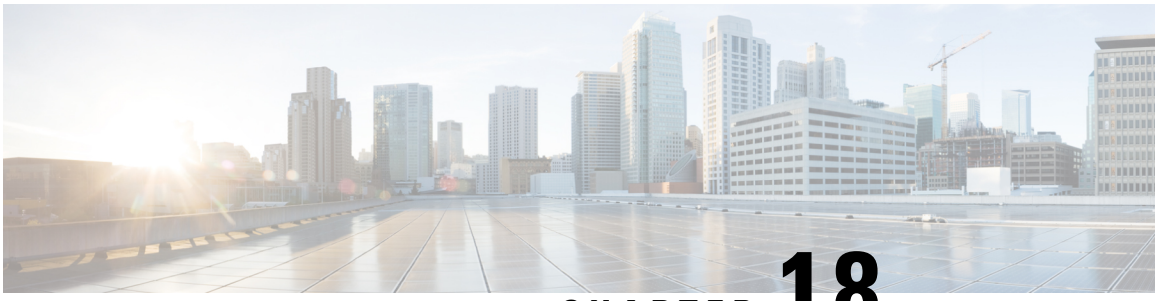
Command Changes

Use the following configuration to enable unauthorized IMSI in the LRR message.

```
configure
  context context_name
    location-service service_name
      slr emergency unauth-imsi
      end
```

NOTES:

- **slr emergency unauth-imsi**: Allows MME to send unauthorized IMSI in the LRR message when available.



CHAPTER 18

P2P Signing Process in StarOS

Feature Summary and Revision History

Summary Data

Applicable Products or Functional Area	StarOS
Applicable Platforms	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *ADC Administration Guide* • *Command Line Interface Reference*

Revision History

Revision Details	Release
First introduced.	21.27

Feature Description

StarOS supports signature file verification along with P2P binary file. This feature is enabled in both trusted and normal builds. Verification is mandatory in trusted builds and is optional in normal builds.

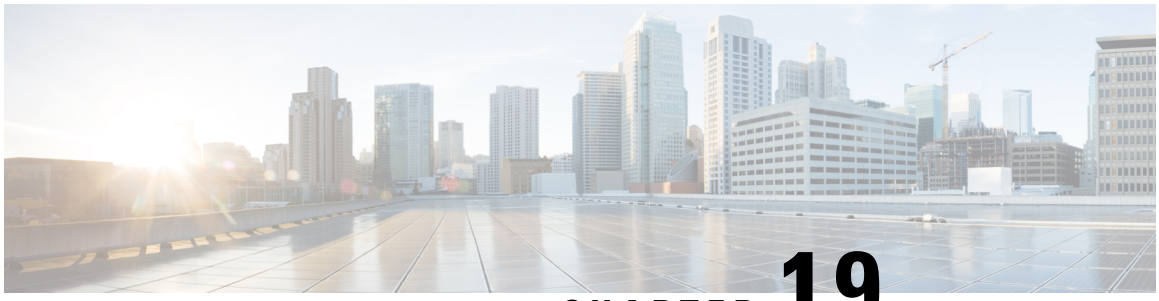
Use the following CLI configuration command to verify the P2P signing process:

```
[local]host_name#
   patch plugin filepath binary_path certificate certificate_path signature
signature_path
```

When P2P binary file along with a signature file gets patched into the system, StarOS verifies the signature and accepts or rejects the P2P binary file.

Relationship to Other Features

P2P signature file verification along with binary file is performed duing Dynamic Software Upgrade For more information, see the *How to perform Dynamic Software Upgrade* section in the *ADC Administration Guide*.



CHAPTER 19

SaMOG Support on VPC-DI

Feature Summary and Revision History

Summary Data

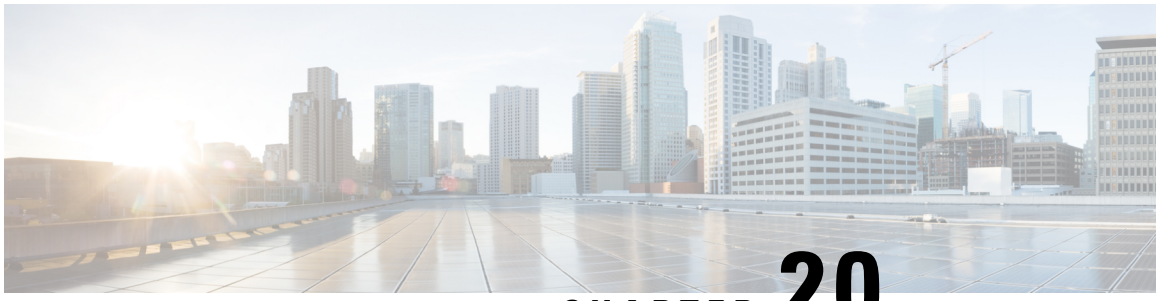
Applicable Product(s) or Functional Area	SaMOG
Applicable Platform(s)	• ASR 5500 • VPC-DI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable.

Revision History

Revision Details	Release
First introduced.	21.27

Feature Description

SaMOG is supported on the VPC-DI platform.



CHAPTER 20

Support for 187 and 188 Information Element Types on S2b Interface

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*ePDG Administration Guide*

Revision History

Revision Details	Release
Support is introduced for inclusion of 187 and 188 Information Element types on S2b Interface.	21.27.m0

Feature Description

During detection and handling of late arriving requests, a GTP-C entity initiates a Create Session Request (ePDG) with the Origination Time Stamp message. This indicates the absolute time at which the request is initiated and the Maximum Wait Time indicating the maximum time to complete the processing of the request. The Maximum Wait Time, together with the Origination Time Stamp, indicates the absolute time at which the request times out at the originating entity. The receiving node utilizes the same time stamp and maximum wait time to identify if it is still a valid message and if it should process it. If the message is processed, the intermediate nodes replicate the time stamp and maximum wait time in messages that are generated by the node toward other peers. Each network element compares the Time Stamp and its own synced Network Time Protocol (NTP) time to ensure that stale messages are not processed.

If any session-related information is created and before the network element responds, the maximum wait time has passed, the network element ensures to clear or release stale session information.

In ePDG, according to the 3GPP 29.274 version, the Origination Time Stamp (188) and Maximum Wait Time (187) Information Element types (IE) are supported into the messages instead of 255 IE type. The feature is only supported for s2b, and s5/s8 interface. P-GW supports receiving and sending the Origination Time Stamp and Max Wait Time IEs / AVPs in these interfaces such a S2b, Gx, and S6b.

How it Works

This section describes the call flow procedures that are related to messages and nodes carrying Origination Time Stamp and Maximum Wait Time (MWT):

The IEs obtained from ePDG send messages toward P-GW, PCRF, and AAA nodes without any modification.

Call Flow

Figure 4: Displays IEs Accross nodes

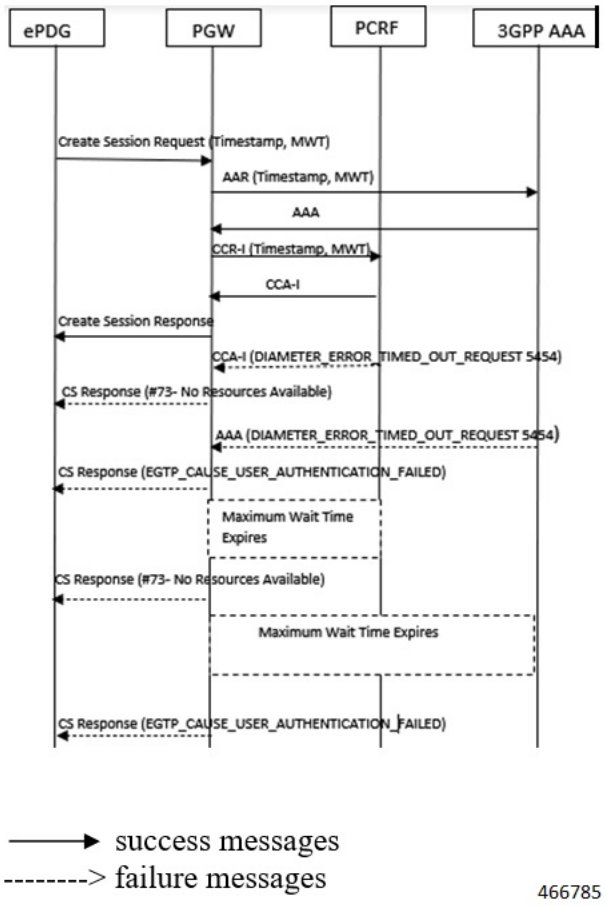


Table 15: Procedure

Step	Message Type	Description
1	Create Session Request	The ePDG includes Origination Time Stamp and Maximum Wait time on S2b interface When present, the Origination Time Stamp contains the Universal Time Code (UTC) time when the originating entity initiated the request, and the Maximum Wait Time contains the duration (number of milliseconds since the Origination Time Stamp) during which the originator of the request waits for a response.
2	Credit Control Request-Initial Request	The IEs received in P-GW will be sending to PCRF through Gx interface. This gets included only in the initial request of CCR.

Step	Message Type	Description
3	Authentication Authorization Request	The IEs received in P-GW sends messages to AAA through s6b interface.

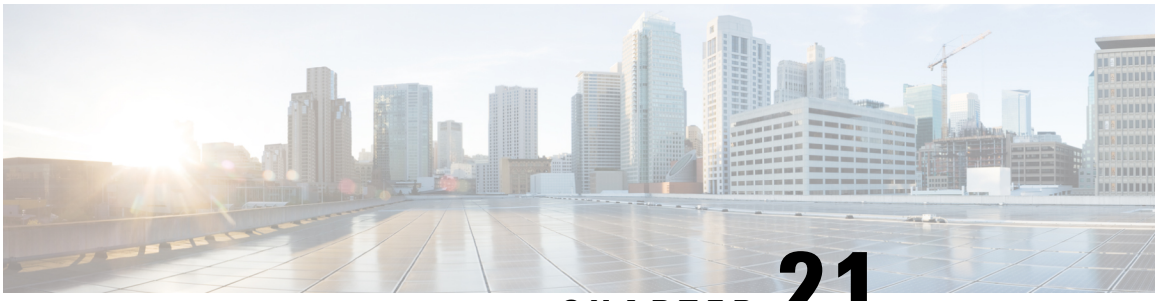
Supported RAT Types

The Origination Time Stamp and Maximum Wait Time IEs are supported for WLAN RAT type. The received IEs in P-GW sends messages on Gx and S6b interfaces.

Handling Handover

Handover (HO) from LTE to WLAN and vice versa is supported to include **Origination Time Stamp and Maximum Wait Time** IEs. During the Handoff from LTE to Wi-Fi or vice versa, the **Origination Time Stamp and Maximum Wait Time** IEs sends messages on S5 and S2b interfaces and not on Gx and S6b interfaces.

In case of LTE to WLAN HO, if a new create session request comes from ePDG, then that request is considered as a new CSR and the handover process is same as the initial attach for new IEs.



CHAPTER 21

Support for 187 and 188 Information Element Types on S5 and S8 Interfaces

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*MME Administration Guide*

Revision History

Revision Details	Release
Support is introduced for inclusion of 187 and 188 Information Element types on S5 and S8 Interfaces.	21.27.m0

Feature Description

During detection and handling of late arriving requests, a GTP-C entity initiates a Create Session Request (MME) with the Origination Time Stamp message. This indicates the absolute time at which the request is initiated and the Maximum Wait Time indicating the maximum time to complete the processing of the request. The Maximum Wait Time, together with the Origination Time Stamp, indicates the absolute time at which the request times out at the originating entity. The receiving node utilizes the same time stamp and maximum wait time to identify if it is still a valid message and if it should process it. If the message is processed, the intermediate nodes replicate the time stamp and maximum wait time in messages that are generated by the node toward other peers. Each network element compares the Time Stamp and its own synced Network Time Protocol (NTP) time to ensure that stale messages are not processed.

If any session-related information is created and before the network element responds, the maximum wait time has passed, the network element ensures to clear or release stale session information.

In MME, according to the 3GPP 29.274 version, the Origination Time Stamp (188) and Maximum Wait Time (187) Information Element types (IE) are supported into the messages instead of the 255 IE type. The feature is only supported for s2b, s5, and s8 interfaces. P-GW supports receiving and sending the Origination Time Stamp and Max Wait Time IEs / AVPs in these interfaces such as S5, Gx, and S6b.

GGSN on Gn/Gp interface is not supported.

How it Works

This section describes the call flow procedures that are related to messages and nodes carrying Origination Time Stamp and Maximum Wait Time (MWT):

The IEs obtained from MME send messages toward P-GW, PCRF, and AAA nodes without any modification.

Call Flow

Figure 5: Displays IEs Accross nodes

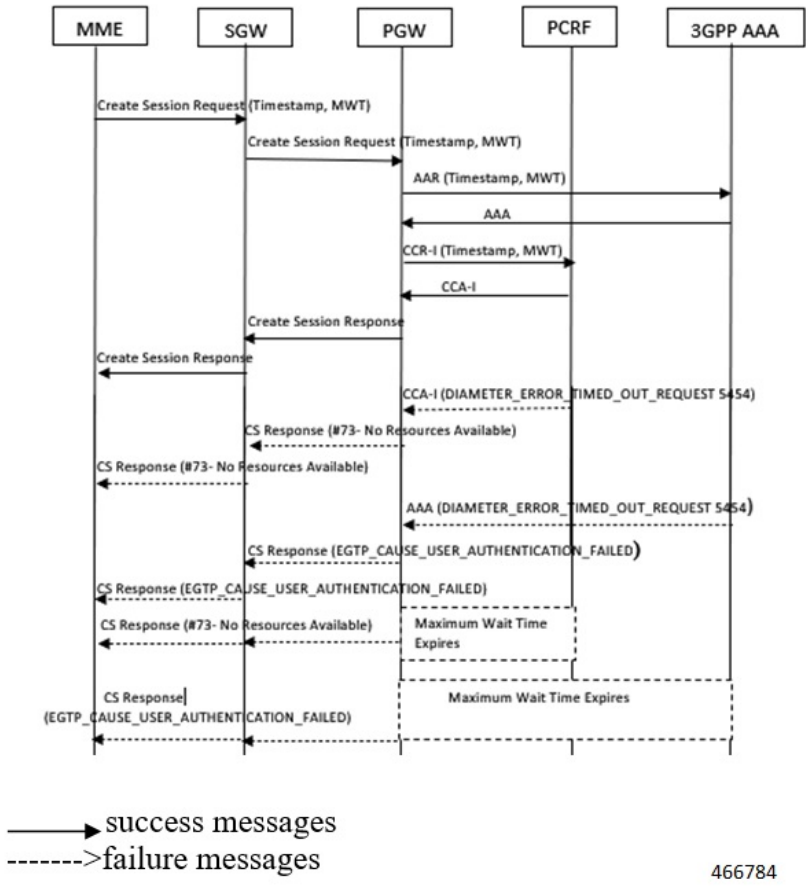


Table 16: Procedure

Step	Message Type	Description
1	Create Session Request	The MME includes Origination Time Stamp and Maximum Wait time on S11 interface. When present, the Origination Time Stamp contain the Universal Time Code (UTC) time when the originating entity initiated the request, and the Maximum Wait Time will contain the duration (number of milliseconds since the Origination Time Stamp) during which the originator of the request waits for a response. If S-GW receives IEs from the MME, then the S-GW includes these IEs on the S5 or S8 interface.
2	Credit Control Request-Initial Request	The IEs received in P-GW sends messages to PCRF through Gx interface. This gets included only in the initial request of CCR.

Step	Message Type	Description
3	Authentication Authorization Request	The IEs received in P-GW sends messages AAA through s6b interface.

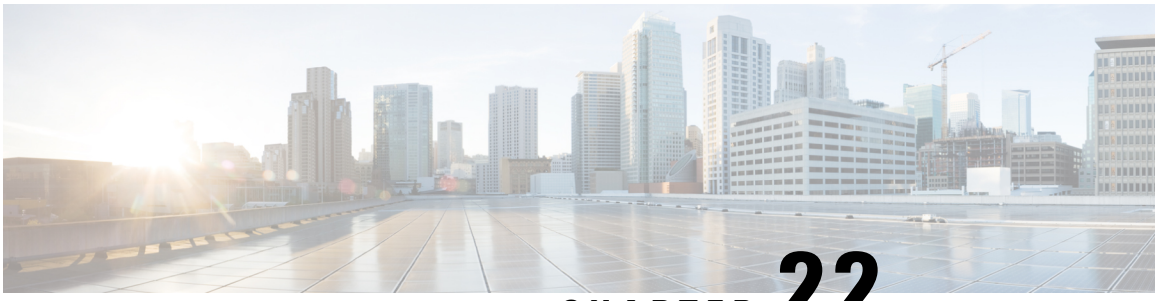
Supported RAT Types

The Origination Time Stamp and Maximum Wait Time IEs are supported for E-UTRAN, NB-IOT and LTE-M RAT types. The received IEs in P-GW sends messages on Gx and S6b interfaces.

Handling Handover

Handover (HO) from LTE to Wi-Fi and vice versa is supported to include **Origination Time Stamp and Maximum Wait Time** IEs. During the Handoff from LTE to Wi-Fi or vice versa, the **Origination Time Stamp and Maximum Wait Time** IEs sends messages on S5 and S2b interfaces and not on Gx and S6b interfaces.

In case of LTE to Wi-Fi HO, if a new create session request comes from ePDG, then that request is considered as a new CSR and the handover process is same as the initial attach for new IEs.



CHAPTER 22

TCP Robustness Compliance with RFC 5961

Feature Summary and Revision History

Summary Data

Applicable Products or Functional Area	P-GW
Applicable Platforms	• ASR 5500 • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *ECS Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.27

Feature Description

P-GW supports TCP Reset (RST) in compliance with RFC 5961. This feature is enabled only when P-GW is in non-proxy mode, and when the connection is in an established state. On receiving the in-sequence TCP RST packets, the P-GW changes the connection to the closed state. This feature supports handling of Out-Of-Sequence (OOS) RST packets in compliance with RFC 5961. Use the **tcp rst-robustness** CLI in the ACS configuration mode to enable the TCP robustness RFC 5961. The feature is disabled by default.

How it Works

When a TCP RST packet comes in established state, the P-GW performs the following actions:

1. If the RST bit is set and the sequence number is outside the current receive window, TCP ignores the segment.
2. If the RST bit is set and the sequence number matches the next expected sequence number (RCV.NXT), TCP must reset the connection.
3. If the RST bit is set and the sequence number does not match the next expected sequence number, despite being within the current receive window, then the RST does not get processed, and a challenge-ack timer starts. The challenge-ack timer is same as the configured 2MSL timer. If the receiver of the OOS RST responds back with a challenge-ack packet, then the timer stops and connection remain in established state. The P-GW closes the connection when the challenge-ack timer expires for RFC 5961 noncompliant TCP endpoint that does not send challenge-ack.

When an attacker injects the OOS RST packet into TCP, the challenge-ack timer starts immediately. The peer sends a challenge-ack, and the challenge-ack timer stops and the connection remains in the established state. If there is no response to the challenge-ack, then the traffic continues to flow.

In both the scenarios, the P-GW does not block the challenge-ack (ACK + RST) and passes it to the remote end.

Configuring TCP RST Robustness

Use the following configuration to configure the TCP RST robustness:

```
configure
          active-charging service acs_service_name
                    rulebase rulebase_name
                    tcp rst-robustness
                    end
```

NOTES:

- **rulebase** *rulebase_name*: Specifies the name of an ACS rulebase to be configured.
- **tcp rst-robustness**: Enables or disables TCP RST robustness as per RFC 5961. By default, TCP RST robustness is disabled.

Monitoring and Troubleshooting

This section provides information to monitor and troubleshoot this feature using show commands.

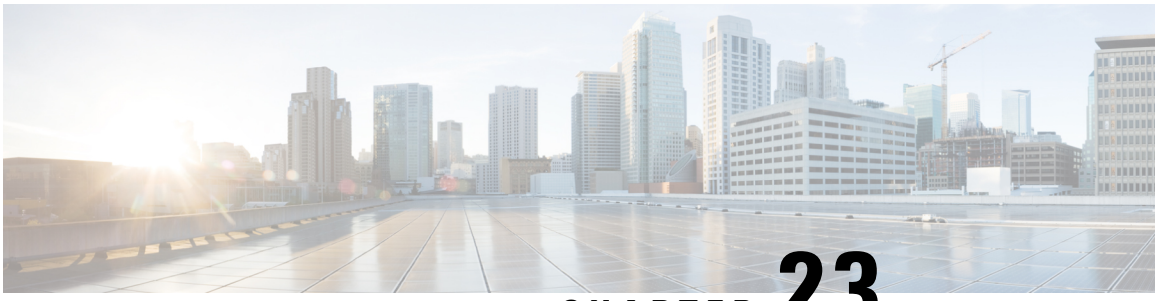
Show Commands and Outputs

This section provides information about the show commands and outputs.

show active-charging analyzer statistics name tcp

Table 17: show active-charging analyzer statistics name tcp Command Output Descriptions

Field	Description
Uplink In Sequence RST Pkts	The total number of uplink in-sequence RST packets received.
Downlink In Sequence RST Pkts	The total number of downlink in-sequence RST packets received.
Uplink Out of Order RST Pkts	The total number of uplink OOS RST packets received.
Downlink Out of Order RST Pkts	The total number of downlink OOS RST packets received.
Uplink Out of Window RST Pkts	The total number of uplinks Out of Window (OOW) RST packets received.
Downlink Out of Window RST Pkts	The total number of downlink OOW RST packets received.
Uplink Challenge-Ack RST Pkts	The total number of uplink challenge-ack packets received
Downlink challenge-ack RST Pkts	The total number of downlink challenge-ack packets received.



CHAPTER 23

Timestamp Accuracy Improvement

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	P-GW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
The **show active-charging flows full debug-info all** command is enhanced to display timestamp accuracy between VPP and session manager. For more information, see the *VPP Metric Enhancement* chapter in the *P-GW Administration Guide.*	21.27

Feature Description

When data packets get offloaded, the calculated ticks from the last arrived packet time lag behind the Starent Network Transmission (SNX) global tick time in the session manager. This results in non-synchronization of time between VPP and session manager. As the flow timeout is deducted incorrectly, the flow gets removed from the session.

The **show active-charging flows full debug-info all** command is enhanced to display the correct flow idle timeout.

Monitoring and Troubleshooting

This section provides information on how to monitor and troubleshoot using show commands available in support of this feature.

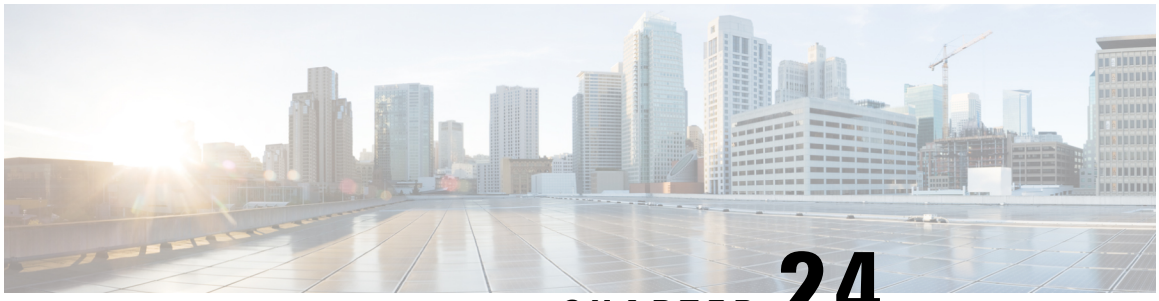
Show Commands and Outputs

This section provides information regarding show commands and their outputs for this feature.

show active-charging flows full debug-info all

Table 18: show active-charging flows full debug-info all Command Output Descriptions

Field	Description
Last Active Tick Time	Specifies the last active tick time for the data packet.
Current Tick Time	Specifies the current system tick time.



CHAPTER 24

VLR Management

This chapter describes various MME features that provide additional resiliency of the Circuit Switched Fallback (CSFB) service, relating to the management of Visitor Location Registers (VLRs).

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	MME
Applicable Platform(s)	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
Support is added for VLR Round-Robin load balancing.	21.27
First introduced	21.22

Feature Description

VLR Management is to manage the subscribers when a specific VLR is offloaded or failed. This chapter explains how MME distributes subscriber to available VLRs during VLR offload or failure.

These features require a valid license key to be installed. Contact your Cisco Account or Support Representative for information on how to obtain a license.

Passive VLR Offloading

The MME provides the ability for an operator to enable or disable "offload" mode for the specified Visitor Locations Registers (VLRs). This capability enables operators to preemptively move subscribers away from an SGs interface associated with a VLR which is planned for maintenance mode. When the **sgs offload**command is set on the MME, all sessions matching this VLR are marked with a "VLR offload" flag. During the next UE activity, the MME requires each UE to perform a combined TAU/LAU. This feature is available to all VLRs, both non-pooled VLRs and those configured within an MME LAC pool area.

The VLR offload functionality and MME offload functionality cannot be activated at the same time.

Active VLR Offloading

Active VLR Offloading provides all of the functionality of Passive VLR Offloading, but also actively detaches UEs associated with the VLR during an operator-specified time period. This expedites the process of offloading UEs prior to a planned VLR maintenance event. This feature is available to all VLRs, both non-pooled VLRs and those configured within an MME LAC pool area.

The VLR offload functionality and MME offload functionality cannot be activated at the same time.

UE Detach on VLR Recovery

The MME supports the ability to perform a controlled release of UEs when a failed VLR becomes active again. This feature is available to all VLRs, both non-pooled VLRs and those configured within an MME LAC pool area.

This applies to UEs that are currently registered as EPS-Only. This enables the UE to return to a combined attached state to restore SMS services.

UE Detach on VLR Failure

The MME supports the ability to perform a controlled release of UEs when an active VLR connection fails. This applies to CSFB UEs that are currently registered to the VLR that failed. This feature is available to all VLRs, both non-pooled VLRs and those configured within an MME LAC pool area.

This enables the UE to return to a combined attached state on a different VLR.

VLR Round-Robin Load Balancing

When multiple VLRs in the same pool are configured in the MME, and when one VLR fails, the subscribers on the failed VLR get attached to only one of the surviving VLRs. As a result, the subscribers are not distributed evenly across the surviving VLRs. The round-robin balancing algorithm is used to distribute subscribers across multiple available VLRs. VLR round-robin load balance is configurable through the CLI.

The MME allocates a VLR in the pool using the Round-robin algorithm for VLR offload (Active and Passive) and VLR failure cases. However, the MME does not use any form of load balancing if the default VLR is configured in pool area through **hash-value non-configured-value use-vlr** *vlr_name*. The default VLR setting takes precedence over the next available or round-robin load balance setting. By default, Round Robin Load Balancing is disabled.

Note The MME displays a warning message, if the default VLR is already configured while trying to configure the VLR Round-robin Load Balancing.

Configuring VLR Offloading

Enabling Passive VLR Offloading

The following Exec mode command instructs the MME to mark UEs associated with the specified VLR with a "VLR offload" flag. This enables the MME to preemptively move subscribers away from an VLR which is scheduled to be put in maintenance mode.

sgs offload sgs-service *service-name* **vlr** *vlr-name* **start time-duration 0 [-noconfirm]**

The following command stops the marking of subscribers associated with the specified VLR to an offload state.

sgs offload sgs-service *service-name* **vlr** *vlr-name* **stop [-noconfirm]**

Notes:

- A **time-duration** value of 0 enables Passive VLR Offloading only.
- More than one VLR may be offloaded at the same time.
- VLR Offloading and MME offloading cannot be performed at the same time.

Enabling Active VLR Offloading

The following Exec mode command instructs the MME to mark UEs associated with the specified VLR with a "VLR offload" flag, and begin detaching these UEs according to the time-duration specified in the command. Affected UEs are detached and required to reattach to another VLR.

sgs offload sgs-service *service-name* **vlr** *vlr-name* **start time-duration** *duration* **[-noconfirm]**

The following command stops active VLR offloading for UEs associated with the specified VLR.

sgs offload sgs-service *service-name* **vlr** *vlr-name* **stop [-noconfirm]**

Notes:

- A **start time-duration** *duration* entry must be an integer from 1 through 3000 to enables Active VLR Offloading and Passive VLR Offloading. The MME splits this time duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers will be actively detached per interval per session manager. For example, a setting of 5 minutes with 600 subscribers in a session manager (from the given VLR) would detach 10 subscribers per 5-second interval. Node level detach rate should be estimated by taking into account the number of session manager tasks. Any subscribers remaining at the expiry of the time-duration will not be detached, but will be marked with the "VLR offload" flag.
- VLR Offloading and MME offloading cannot be performed at the same time.

Configuring VLR Round-Robin Load Balance

Use the following configuration to enable VLR round-robin load balance:

```
configure
   context context_name
     sgs-service sgs_svc_name
         offload method { round-robin |  next-available }
        end
```

NOTES:

- **sgs-service** *sgs_svc_name*: Configures the SGs Service.
- **offload method { round-robin | next-available }**: Configures the round-robin or next-available load balancing method for affected sessions during VLR offload or failure.

Verifying VLR Offload Status and Configuration

The following command displays VLR offload statistics for the specified SGs service.

show sgs-service offload-status service-name *sgs_svc_name*

The following sample output shows VLR Offload related statistics.

```
show sgs-service offload-status service-name sgssvc
VLR Name                 : vlr1
VLR Offload              : Yes
Offloaded Count          : 31678
Total Count              : 43051
VLR Name                 : vlr2
VLR Offload              : No
```

```
Offloaded Count           : 0
Total Count               : 45789
```

To clear the counters displayed by the previous command, issue the following command.

clear sgs-service offload-status service-name *sgs_svc_name*

When Passive or Active VLR Offload is enabled, the following command displays the "VLR Offload" flag for the specified VLR.

show mme-service session vlr-name *vlr_name*

The following output shows the VLR Offload flag enabled.

```
show mme-service session vlr-name vlr1
   CSFB Information:
        SGS Assoc State:    SGs-ASSOCIATED
        SGS Service:        sgssvc
        VLR:                vlr1
        LAI:                123:456:200
        Pool Area:          pool1
        Non-Pool Area:      N/A
        P-TMSI:             0x1
        Flags:
   VLR Reliable Indicator
   VLR Offload
```

The following command shows the offload state of all VLRs on the system.

show sgs-service vlr-status full

```
show sgs-service vlr-status full
MMEMGR                        : Instance 6
MME Reset                     : Yes
Service ID                    : 2
Peer ID                       : 100794369
VLR Name                      : vlr1
SGS Service Name              : test
SGS Service Address           : 192.60.60.25
SGS Service Port              : 29118
VLR IP Address                : 192.60.60.6
VLR Psgsort                   : 29118
Assoc State                   : DOWN
Assoc State Up Count          : 2
VLR Offload                   : No
```

To clear the counters displayed by the previous command, issue either of the following commands. The first command clears statistics for all VLRs, while the second command clears statistics for the specified VLR only.

clear sgs-service vlr-status service-name *sgs_svc_name*
clear sgs-service vlr-status vlr-name *vlr_name*

Enabling UE Detach on VLR Failure or VLR Recover

UE Detach on VLR Recovery

The following Exec mode command instructs the MME to automatically perform active recovery of UEs when a failed VLR becomes responsive again.

sgs vlr-recover sgs-service *sgs_svc_name* **duration** *duration* **backoff-timer** *time* **[-noconfirm]**

Notes:

- When this command is issued, the MME monitors the availability of all VLRs. If a failed VLR become available again, the MME attempts to recover UEs that failed while the VLR was unavailable with an EPS Detach.
- When a VLR is down, and a UE needs to associate with the VLR that went down, the UE will be downgraded to EPS-Only-Attach when initially attaching. This command should be issued after the VLR recovers.
- UEs which required CSFB (voice) and were downgraded as a result of the VLR being down will not be affected by this command. This command remains active until it is disabled with the **no sgs vlr-recover** command.
- **duration** *duration* Specifies the number of minutes during which all qualifying UEs will be recovered.

  The MME splits this duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers are processed per interval per session manager. For example, a setting of 5 minutes with 600 subscribers in a session manager (from a given VLR) would result in the session manager processing 10 subscribers per 5-second interval. Node level detach rate should be estimated by taking into account the number of session manager tasks. Any subscribers remaining at the expiry of the duration will not be processed.
- **backoff-timer** *time* Specifies the number of seconds that the MME will wait, following the detection of a recovered VLR, before starting the VLR recovery actions.
- Refer to the *sgs vlr-recover* command in the Exec Mode chapter of the *Command Line Interface Reference* for more information.

The command listed below disables the **sgs vlr-recover** functionality.

no sgs vlr-recover sgs-service *sgs_svc_name* **[-noconfirm]**

UE Detach on VLR Failure

Manually Enabling UE Detach on VLR Failure

The following Exec mode command instructs the MME to perform controlled release of CSFB UEs connected to a VLR when a VLR becomes unavailable.

sgs vlr-failure sgs-service *sgs_svc_name* **duration** *duratioin* **backoff-timer** *time* **[-noconfirm]**

Notes:

- When enabled, the MME monitors the availability of all VLRs. If one or more VLRs become unavailable, the MME performs a controlled release (EPS IMSI detach) for all UEs associated with that VLR. If another VLR is available, the MME sends a combined TA/LA Update with IMSI attach.
- **duration** *duration* Specifies the number of minutes during which all qualifying UEs will be detached. Enter an integer from 1 to 3000.

  The MME splits this duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers are processed per interval by each session manager. For example, a setting of 5 minutes with 600 subscribers in a session manager (from a given VLR) would result in the session manager processing 10 subscribers per

5-second interval. Node level detach rate should be estimated by taking into account the number of session manager tasks. Any subscribers remaining at the expiry of the duration will not be processed.

- **backoff-timer** *time* Specifies the number of seconds the MME will wait following the detection of a VLR condition before starting the controlled release of affected UEs. Enter an integer from 1 through 3000.

The enabling command remains active until it is disabled with the following command:

no sgs vlr-failure sgs-service *sgs_svc_name* **[-noconfirm]**

Refer to the **sgs vlr-failure** command in the *Exec Mode (D-S)* chapter of the *Command Line Interface Reference* for more information.

Verifying UE Detach on VLR Failure/Recovery Status and Configuration

Use the following command to display the offload status of all VLRs on the system.

show sgs-service vlr-status full

This sample output shows the fields relating to UE Detach on VLR Failure and UE Detach on VLR Recover. Not all fields shown below may be displayed, based on your configuration:

```
show sgs-service vlr-status full
Exec Configured VLR Failure Detach : No         Detached Count : 0        Total : 0
```

To clear the counters displayed by the previous command, issue either of the following commands. The first command clears statistics for all VLRs for the specified SG, while the second command clears statistics for the specified VLR only.

clear sgs-service vlr-status service-name *sgs_svc_name*
clear sgs-service vlr-status vlr-name *vlr_name*

Monitoring and Troubleshooting VLR Offload

SNMP Traps

The following traps are generated to track conditions relating to VLR associations:

The VLR down trap is raised only after the VLR goes to the DOWN state after being UP. When all VLR's are down after at least one has been UP, the all VLR's DOWN trap is raised.

- **starVLRAssocDown** and **starVLRAssocUp** - indicates a condition when an association of a VLR is down (VLRAssocDown), and when a down association comes back up (VLRAssocUp).
- **starVLRAllAssocDown** and **starVLRAllAssocDownClear** - indicates a condition when **all** SCTP associations of **all** VLRs are down (VLRAllAssocDown), and when a down association comes back up (VLRAllAssocDownClear).

Bulk Statistics

This SGs schema provides operational statistics that can be used for monitoring and troubleshooting the SGs connections on a per-VLR basis.

Refer to the *SGs Schema Statistics* chapter of the *Statistics and Counters Reference* for detailed explanations of all bulk statistics provided in this schema.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs.

VLR Offload Status

The following command shows the status of the VLR offload process for the specified SGs service.

show sgs-service offload-status service-name *sgs_svc_name*

The following command shows the status and configuration information of all VLRs on the system.

show sgs-service vlr-status full

UE Detach on VLR Recovery and VLR Failure

The following command shows the statistics resulting from the **sgs vlr-recover** and **sgs vlr-failure** commands.

show sgs-service vlr-status full

Refer to the *show sgs-service* chapter of the *Statistics and Counters Reference* for detailed explanations of all information displayed by this command.