Release Change Reference, StarOS Release 21.23

First Published: 2021-03-31

Last Modified: 2022-03-15

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

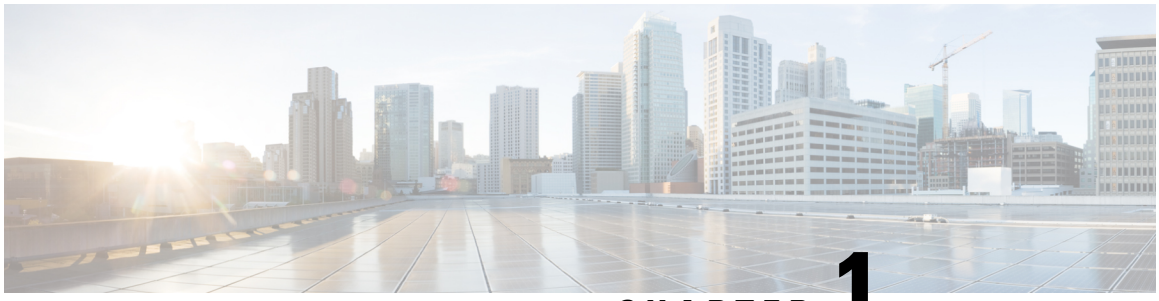
Conventions Used

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

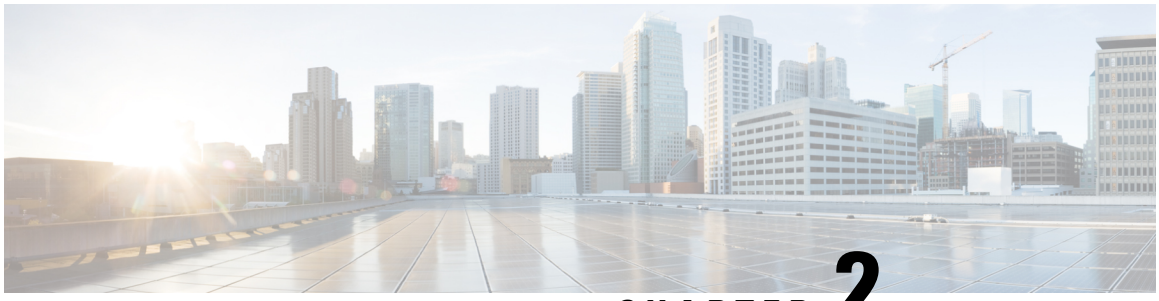
Release 21.23 Features and Changes Quick Reference

Release 21.23 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
APN, QCI, and ARP-based DSCP Mapping for WPS Sessions, on page 31	P-GW	21.23
Capability to Record and Produce Call Transactions, on page 57	ePDG	21.23
Cisco Ultra Traffic Optimization Bulk Statistics Enhancements, on page 63	P-GW	21.23
Closed Subscriber Group Mobility Event Support on P-GW and GGSN, on page 67	P-GW	21.23
Crowd Sourcing Optimization, on page 75	P-GW	21.23
Customizing Last User Location Information	• P-GW • SAEGW	21.23.14
Customizing TAC Field in CDR	• P-GW • SAEGW	21.23.14
Diameter Route Table Entries Display Limit and Filtration Enhancement , on page 89	• P-GW • SGW • SAEGW • GGSN	21.23.12

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Dynamic Enabling of UBR Buffering in MME Services, on page 91	MME	21.23.20
Enhanced Event Logging, on page 93	MME	21.23.1
Extraction of IPv4 Addresses Embedded in IPv6 Addresses, on page 109	ECS	21.23
Failure Counters for CSFB MT Counters	MME	21.23
Gy Interface Specification for Compliance 2019, on page 119	P-GW	21.23
IMS PCO Configurations when Gx is Down, on page 125	P-GW	21.23
Increasing Maximum Chunks Per User NAPT for 5G MiFi, on page 131	NAT	21.23
Inter-MME Handover for Modify Bearer Requests without S11-U TEID, on page 133	P-GW	21.23
MME Masked IMEISV	MME	21.23
MME Bearer Request Message Enhancements During Handover Process , on page 141	MME	21.23.20
Mobile Hotspot Usage on RADIUS Accounting, on page 143	P-GW	21.23
4G Network Upgrade on Gx Interface	P-GW	21.23
Password Expiration Notification, on page 149	P-GW	21.23
P-GW Buffering Optimization, on page 155	P-GW	21.23
P-GW Buffering Mechanism, on page 153	P-GW	21.23
PLMN Level Statistics for ePDG Services, on page 159	ePDG	21.23
PLMN Level Statistics for SaMOG Services, on page 171	SaMOG	21.23
Separation of 2G 3G 4G WLAN Bulkstatistics, on page 187	P-GW	21.23
Sessmgr Restart While Processing Secondary RAT Usage CDR Records, on page 207	P-GW	21.23

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Secondary RAT Usage Report in CDR Records, on page 197	• P-GW • SAEGW • S-GW	21.23.14
Suppressing Handover Request for VoWiFi IR Subscribers , on page 211	ePDG	21.23
Support to Add Two Additional Attributes in EDR, on page 209	MME	21.23
Timeout Exclusion from CSFB Counters	MME	21.23



CHAPTER 2

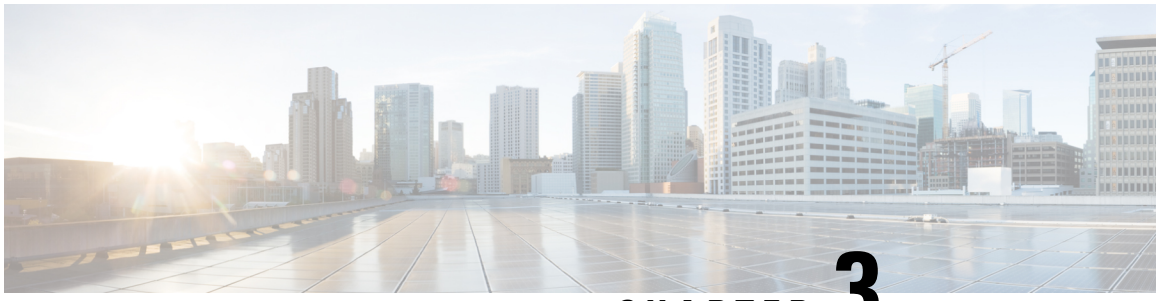
Feature Defaults Quick Reference

Feature Defaults

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

Feature	Default
APN, QCI, and ARP-based DSCP Mapping for WPS Sessions	Disabled - Configuration Required
Capability to Record and Produce Call Transactions on ePDG	Disabled - Configuration Required
Cisco Ultra Traffic Optimization Bulk Statistics Enhancements	Disabled - Configuration Required
Closed Subscriber Groups Mobility Event Support on P-GW and GGSN	Disabled - Configuration Required
Crowd Sourcing Optimization	Disabled - Configuration Required
Customizing Last User Location Information	Disabled - Configuration Required
Customizing TAC Field in CDR	Disabled - Configuration Required
Enhanced Event Logging	Enabled - Always-on
Diameter Route Table Entries Display Limit and Filtration Enhancement	Not Applicable
Dynamic Enabling of UBR Buffering in MME Services	Disabled - Configuration Required
Extraction of IPv4 Addresses Embedded in IPv6 Addresses	Disabled - License Required
Failure Counters for CSFB MT Counters	Enabled - Always-on
Gy Interface Spec Compliance 2019	Disabled - Configuration Required
IMS PCO Configurations when Gx is Down	Disabled - Configuration Required
Increasing Maximum Chunks Per User NAPT for 5G MiFi	Disabled - Configuration Required

Feature	Default
Inter-MME Handover for Modify Bearer Requests without S11-U TEID	Disabled - Configuration Required
MME Masked IMEISV	Disabled - Configuration Required
MME Bearer Request Message Enhancements During Handover Process	Disabled - Configuration Required
Mobile Hot Spot Usage on RADIUS Accounting	Disabled - Configuration Required
4G Network Upgrade Gx Interface	Disabled - Configuration Required
Password Expiration Notification	Enabled - Always-on
P-GW Buffering Mechanism	Enabled - Configuration Required
P-GW Buffering Optimization	Enabled - Always-on
PLMN Level Statistics for ePDG Services	Disabled - Configuration Required
PLMN Level Statistics for SaMOG Services	Disabled - Configuration Required
Separation of 2G 3G 4G and WLAN Bulkstatistics	Disabled - Configuration Required
Sessmgr Restart While Processing Secondary RAT Usage CDR Records	Enabled - Configuration Required
Secondary RAT Usage Report in CDR Records	Disabled - Configuration Required
Suppressing Handover Request for VoWiFi IR Subscribers	Disabled - Configuration Required
Support to Add Two Additional Attributes in EDR	Enabled - Always-on
Timeout Exclusion from CSFB Counters	Enabled - Always-on



CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.23 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 21.23 include:

- New Bulk Statiscs, on page 7
- Deprecated Bulk Statistics, on page 20
- Modified Bulk Statistics, on page 21

New Bulk Statiscs

APN Schema

The following bulk statistics are added in the APN schema to support the 2G, 3G, 4G, WLAN bulkstats separation feature:

Counters	Description
uplnk-bytes-gtpv2-s2a	Indicates the total number of bytes sent from the APN for a GTPV2 based S2A RAT type towards the Internet/PDN on the Gi interface.
dnlnk-bytes-gtpv2-s2a	Indicates the total number of bytes received for a GTPV2 based S2A RAT type on the Gi interface for the APN.
uplnk-bytes-gtpv2-s2b	Indicates the total number of bytes sent from the APN for a GTPV2 based S2B RAT type towards the Internet/PDN on the Gi interface.
dnlnk-bytes-gtpv2-s2b	Indicates the total number of bytes received for a GTPV2 based S2B RAT type on the Gi interface for the APN.

dyn-ipv4-success-eutran	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a EUTRAN RAT type.
dyn-ipv4-success-gtpv2-s2a	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2A RAT type.
dyn-ipv4-success-gtpv2-s2b	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2B RAT type.
dyn-ipv6-success-eutran	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a EUTRAN RAT type.
dyn-ipv6-success-gtpv2-s2a	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2A RAT type
dyn-ipv6-success-gtpv2-s2b	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2B RAT type.
dyn-ipv4v6-success-eutran	Indicates the total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a EUTRAN RAT type.
dyn-ipv4v6-success-gtpv2-s2a	Indicates the total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2A RAT type.
dyn-ipv4v6-success-gtpv2-s2b	The total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2B RAT type.
upc-rx-geran	Indicates the total number of Update PDP Context Request messages received from the SGSN(s) for a GERAN RAT type per APN.
upc-tx-geran	Indicates the total number of Update PDP Context Request messages sent to the SGSN(s) for a GERAN RAT type per APN.
upc-rx-accept-geran	Indicates the total number of Update PDP Context Response messages received from SGSN(s) containing a cause value of 128 (80H, Request accepted) for a GERAN RAT type per APN.

upc-tx-accept-geran	Indicates the total number of Update PDP Context Response messages sent to the SGSN(s) containing a cause value of 128 (80H, Request accepted) for a GERAN RAT type per APN.
upc-rx-utran	Indicates the total number of Update PDP Context Request messages received from the SGSN(s) for a UTRAN RAT type per APN.
upc-tx-utran	Indicates the total number of Update PDP Context Request messages sent to the SGSN(s) for a UTRAN RAT type per APN.
upc-rx-accept-utran	Indicates the total number of Update PDP Context Response messages received from SGSN(s) containing a cause value of 128 (80H, Request accepted) for a UTRAN RAT type per APN.
upc-tx-accept-utran	Indicates the total number of Update PDP Context Response messages sent to the SGSN(s) containing a cause value of 128 (80H, Request accepted) for a UTRAN RAT type per APN.
cpc-accept-geran	Indicates the total number of Create PDP Context Response messages transmitted containing a cause value of 128 (80H, Request accepted)for a GERAN RAT type per APN.
cpc-accept-utran	Indicates the total number of Create PDP Context Response messages transmitted containing a cause value of 128 (80H, Request accepted) for a UTRAN RAT type per APN.
cpc-nomem-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 212 (D4H, No memory is available) for a GERAN RAT type per APN.
cpc-nomem-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 212 (D4H, No memory is available) for a UTRAN RAT type per APN.
cpc-noresource-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 199 (C7H, No resources available) for a GERAN RAT type per APN.

cpc-noresource-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 199 (C7H, No resources available) for a UTRAN RAT type per APN.
cpc-srv-not-supp-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 200 (C8H, service not Supported) for a GERAN RAT type per APN.
cpc-srv-not-supp-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 200 (C8H, service not Supported) for a UTRAN RAT type per APN.
cpc-sys-fail-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 204 (CCH, System failure) for a GERAN RAT type per APN.
cpc-sys-fail-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 204 (CCH, System failure) for a UTRAN RAT type per APN.
cpc-auth-fail-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 209 for a GERAN RAT type per APN.
cpc-auth-fail-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 209 for a UTRAN RAT type per APN.
cpc-no-apn-subscription-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent for a GERAN RAT type per APN because there was no apn subscription.
cpc-no-apn-subscription-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent for a UTRAN RAT type per APN because there was no apn subscription.
cpc-missing-apn-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 219 (DBH, Missing or unknown APN) for a GERAN RAT type per APN.

cpc-missing-apn-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 219 (DBH, Missing or unknown APN) for a UTRAN RAT type per APN.
cpc-addr-occupied-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 211 (D3H, All dynamic PDP addresses are occupied) for a GERAN RAT type per APN.
cpc-addr-occupied-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 211 (D3H, All dynamic PDP addresses are occupied) for a UTRAN RAT type per APN.

DPCA-IMSA Schema

The following bulk statistics are added in the DPCA-IMSA Schema to support Statistics of overlapping and time-out request.

Counters	Description
dpca-imsa-exp-late-overlapping-request	Displays the total number of times the diameter experimental result code DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST(5453) is received in CCA message.
dpca-imsa-exp-timed-out-request	Displays the total number of times the diameter experimental result code DIAMETER_ERROR_TIME_OUT_REQUEST(5454) is received in CCA message.

eGTP-C Schema

The following new bulk statistics variables are added to the eGTP-C schema in support of APN, QCI, and ARP-based DSCP Mapping for WPS Sessions feature. These statistics are only for the current bulkstat intervals.

Note This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.

Counters	Description
s11-tun-recv-modbearerreq-wps	Shows the total number of tunnel modify bearer request messages received by the system for WPS subscriber on the s11 interface.
s11-tun-sent-modbearerresp-wps	Shows the total number of tunnel modify bearer response messages sent by the system for WPS subscriber on the s11 interface.

Counters	Description
s11-tun-sent-crebearerreq-wps	Shows the total number of tunnel create bearer request messages sent by the system for WPS subscriber on the s11 interface.
s11-tun-recv-crebearerresp-wps	Shows the total number of tunnel create bearer response messages received by the system for WPS subscriber on the s11 interface.
s11-tun-sent-updbearerreq-wps	Shows the total number of tunnel update bearer request messages sent by the system for WPS subscriber on the s11 interface s11.
s11-tun-recv-updbearerresp-wps	Shows the total number of tunnel update bearer response messages received by the system for WPS subscriber on the s11 interface .
tun-sent-cresessreq-wps	Shows the total number of tunnel create session request messages sent by the system for WPS subscriber on the S5/S8 interface .
tun-recv-updbearerresp-wps	Shows the total number of tunnel update bearer response messages received by the system for WPS subscriber on the S5/S8 interface.
tun-sent-updbearerresp-wps	Shows the total number of tunnel update bearer response messages sent by the system for WPS subscriber on the S5/S8 interface .

epdg-plmn schema

The following bulk statistics are added in the epdg-plmn-schema to support Bulk Statistics Variables.

Counters	Description
plmn-mcc	The PLMN MCC for which this statistics is collected. This is a key variable.
plmn-mnc	The PLMN MNC for which this statistics is collected. This is a key variable.
plmn-totsetup-success	Indicates that total setup success.
plmn-tot-success-handoff	Indicates that total number of successful LTE to Wi-Fi handoffs.
plmn-tot-handoff-attempts	Indicates that total number of LTE to Wi-Fi handoff attempts.
plmn-totsetup-attempt	Indicates that total setup attempt.
plmn-totattempt-failure	Indicates that total failure attempts.
plmn-totgtp-curr-ue-in-sys	Indicates that total GTP active UEs in the system.
plmn-curses	Indicates that total number of current ePDG sessions.
plmn-tot-success-handoff	Indicates that total number of successful handoff sessions.

Counters	Description
plmn-pgw-fallback-succeeded	Indicates that total number of P-GW Fallback sessions succeeded.
plmn-pgw-fallback-attempted	Indicates that total number of P-GW Fallback sessions attempted.
plmn-reauthor-success	Indicates that total number of reauthorization success messages.
plmn-reauthor-attempt	Indicates that total number of reauthorization attempted messages.
plmn-eap-rxsuccsrvrpassthru	Indicates that total number of successful EAP server statistics received on pass through mode.
plmn-eap-rxttlsrvrpassthru	Indicates that total number of EAP server statistics received on pass through mode.
plmn-sess-disconnect-remote	Indicates that total number of Remote disconnect sessions at PLMN level.
plmn-sess-disconnect-admin	Indicates that total number of Administrator disconnect sessions at PLMN level.
plmn-sess-disconnect-idle-timeout	Indicates that total number of disconnect sessions due to idle timeout reasons.
plmn-sess-disconnect-abs-timeout	Indicates that total number of disconnect sessions due to absolute timeout reasons.
plmn-sess-disconnect-longdur-timeout	Indicates that total number of disconnect sessions due to long duration timeout.
plmn-sess-disconnect-sesssetup-timeout	Indicates that total number of session disconnects due to setup timeout.
plmn-sess-disconnect-noresource	Indicates that total number of session disconnects due to non-availability of resources.
plmn-sess-disconnect-authfail	Indicates that total number of session disconnects due to authentication failure.
plmn-sess-disconnect-flowadd-failure	Indicates that total number of session disconnects due to flow add failure.
plmn-sess-disconnect-invalid-dest	Indicates that total number of session disconnects due to invalid destination context.
plmn-sess-disconnect-srcaddr-violation	Indicates that total number of session disconnects due to source address violation.
plmn-sess-disconnect-lmarevoc	Indicates that total number of session disconnects due to LMA revocation.

Counters	Description
plmn-sess-disconnect-dupreq	Indicates that total number of session disconnects due to duplicate requests.
plmn-sess-disconnect-addrassign-failure	Indicates that total number of sessions disconnects due to address assignation failure.
plmn-sess-disconnect-handoff	Indicates that total number of sessions disconnects due to LTE and other handoff
plmn-sess-disconnect-misc	Indicates that total number of session disconnects due to miscellaneous reasons.
plmn-ikev2-auth-p1succ	Indicates that total number of IKEv2 authentication phase 1 success messages.
plmn-ikev2-auth-p1req	Indicates that total number of IKEv2 authentication phase 1 request messages.
plmn-ikev2-auth-p1fail	Indicates that total number of IKEv2 authentication phase 1 failure messages.
plmn-ikev2-ikesadelrep-recv	Indicates that total number of IKEv2 SA delete request received.
plmn-ikev2-ikesadelrep-sent	Indicates that total number of IKEv2 SA delete requests sent.
plmn-der-req-id-sent	Indicates total number of DER messages transmitted.
plmn-dea-chal-rcvd	Indicates that total number of DEA Challenge messages received.
plmn-dea-acpt-rcvd	Indicates that total number of DEA Accept messages received.
plmn-diamauth-msg-rar	Indicates that total number of RAR messages received.
plmn-diamauth-msg-raa	Indicates that total number of RAA messages transmitted.
plmn-diamauth-msg-asr	Indicates that total number of ASR messages received.
plmn-diamauth-msg-asa	Indicates that total number of ASA messages transmitted.
plmn-diamauth-msg-str	Indicates that total number of STR messages transmitted.
plmn-totgtp-attempt	.Indicates total number of GTP attempts on S2b interface.
plmn-totgtp-success	Indicates that total number of successful GTP sessions on S2b interface.

Counters	Description
plmn-totgtp-failure	IndiccateDisplays total number of failed GTP sessions
plmn-tun-recv-crebear	Indicates that total number of Create Bearer Request messages received.
plmn-tun-sent-crebearrespaccept	Indicates that total number of Create Bearer Response Accepted messages transmitted.
plmn-tun-recv-crebearDiscard	Indicates that total number of Create Bearer Request Discarded messages received.
plmn-tun-sent-crebearres	Indicates that total number of Create Bearer Response transmitted.
plmn-tun-sent-crebearrespdenied	Indicates that total number of Create Bearer Response Denied messages transmitted.
plmn-tun-sent-delsessreq	Indicates that total number of Delete session requests transmitted.
plmn-tun-recv-delsessrespaccept	Indicates that total number of Delete session response accepted messages received.

samog-plmn-schema

The following bulk statistics are added in the samog-plmn-schema to support Bulk Statistics Variables.

Counters	Description
plmn-mcc	The PLMN MCC context configured at the PLMN level that is currently facilitating the SaMOG Service. This is a key variable.
plmn-mnc	The PLMN MNC context configured at the PLMN level that is currently facilitating the SaMOG service. This is a key variable.
plmn-mrme-access-mode-gtpv2-selected	Indicates that the Network access mode statistics for the selected gtpv2 interface.
plmn-mrme-eap-call-attempted	Indicates that the total number of MRME EAP Session Attempted.
plmn-mrme-eap-call-success	Indicates that the total number of successful MRME EAP sessions.
plmn-mrme-eap-call-failure	Indicates that the total number of failed MRME EAP sessions.
plmn-mrme-eap-call-current	Indicates that the total number of current MRME EAP sessions.
plmn-cgw-sessstat-pdns-gtpv2-active	Indicates that the total number of session statistics active for PDN gtpv2 interface.
plmn-dhcp-curservsess	Indicates that the total number of DHCP server sessions that are active.
plmn-sess-total-setup	Indicates that the total number of DHCP Sessions setup.

Counters	Description
plmn-total-released	Indicates that the total number of DHCP sessions released.
plmn-dhcp-msg-discover-rx	Indicates that the total number of DHCP discover messages received.
plmn-dhcp-msg-offer-tx	Indicates that the total number of DHCP offer messages transmitted.
plmn-dhcp-msg-request-rx	Indicates that the total number of DHCP request messages received.
plmn-dhcp-msg-ack-tx	Indicates that the total number of DHCP acknowledgment messages transmitted.
plmn-dhcp-msg-nak-tx	Indicates that the total number of transmitted DHCP messages that are not acknowledged.
plmn-cgw-sessstat-ipv6-router-advt-sent	Indicates that the total number of router advertisement messages sent.
plmn-tun-sent-cresess	Indicates the total number of Create Sessions Request Initially transmitted.
plmn-tun-recv-cresessrespaccept	Indicates that the total number of Create Session Response Accepted messages received.
plmn-tun-recv-crebear	Indicates that the total number of Create Bearer Requests Initial messages received.
plmn-tun-sent-crebearrespaccept	Indicates that the total number of Create Bearer Response Accepted messages transmitted.
plmn-tun-sent-delsessreq	Indicates that the total number of Delete Session Request Initial messages transmitted.
plmn-tun-recv-delsessrespaccept	Indicates that the total number of Delete Session Response Accepted messages received.
plmn-tun-recv-delbearreq	Indicates that the total number of Delete Bearer Request Initial messages received.
plmn-tun-sent-delbearrespaccept	Indicates that the total number of Delete Bearer Response Accepted messages transmitted.
plmn-der-req-id-sent	Indicates the total number of DE Requests.
plmn-dea-chal-rcvd	Indicates that the total number of DEA Challenge statistics received.
plmn-dea-acpt-rcvd	Indicates that the total number of DEA Accept statistics received.
plmn-diamauth-msg-asr	Indicates that the total number of Diameter authentication messages are received for ASR.

Counters	Description
plmn-diamauth-msg-asa	Indicates the total number of Diameter authentication messages received for ASA.
plmn-diamauth-msg-rar	Indicates the total number of Diameter authentication messages received for RAR.
plmn-diamauth-msg-raa	Indicates that the total number of Diameter authentication messages for RAA.
plmn-diamauth-msg-str	Indicates that the total number of Diameter authentication messages are received for STR.
plmn-diamauth-msg-sta	Indicates that the total number of Diameter authentication messages are received for STA.
plmn-acc-req-sent	Indicates that the total number of PLMN accounting requests sent.
plmn-acc-rsp-rcvd	Indicates that the total number of PLMN accounting responses are received.
plmn-acc-start-sent	Indicates that the total number of PLMN accounting start messages are sent.
plmn-acc-stop-sent	Indicates that the total number of PLMN accounting stop messages sent.
plmn-acc-req-timeout	Indicates that the total number of PLMN accounting requests timed out.

MT Voice CSFB

The following bulk statistics are added in the MT Voice CSFB to support Bulk Statistics Variables.

Counters	Description
csfb-mt-voice-sgs-paging-request	This counter records all non-retransmitted SGS Paging Requests rx'd from MSC (i.e. The starting point of all the MT CSFB Voice procedures both Idle and Active modes).
csfb-mt-voice-failure-paging-timeout	This counter records max re-transmission timeout failure when eNB/UE do not respond to MME paging request (Idle mode error).
csfb-mt-voice-failure-miscellaneous	This counter records miscellaneous internal errors such as software errors, internal non-delivery errors, internal aborts, message validation errors, collision with start of MO Voice CSFB procedure etc (i.e. Errors not directly linked to the 3GPP spec procedures).

csfb-mt-voice-failure-ext-srv-req-reject	This counter records the failure when the cause code in the Extended Service Request is NOT CSFB Accept (Idle and Active modes).
csfb-mt-voice-failure-init-ctxt-setup	This counter records any Initial Context Setup Response failures encountered during the Idle mode scenario.
csfb-mt-voice-failure-cs-notification	This counter records non-delivery/max-retransmission timeout of the CS NOTIFICATION to the UE (Active mode scenario).
csfb-mt-voice-failure-ue-ctxt-mod	This counter records any UE Context Modification failures (either timeout or failure response - Active mode).
csfb-mt-voice-failure-sgs-service-abort-req	This counter records any procedure aborts based on the MT Voice Cancelled flag which is set when rx'ing the SGS service Abort Request from the MSC/VLR.
csfb-mt-voice-failure-ue-ctxt-rel-misc	This counter records any other S1 UE Context Release error or cause code that doesn't equal "cs-fallback-triggered = 23" but not the other cause codes stated above (Active mode no HO).
csfb-mt-voice-success-ue-ctxt-rel	This counter records the final success when a S1 UE Context Release response has cause-code "cs-fallback-triggered=23" (Active mode no HO). Successful end-point of the MT CSFB Voice with no HO.

IMSA Schema

The following bulk statistics are included in the IMSA Schema to track high and low priority categories for WPS and Non-WPS users for the APN, QCI, and ARP-based DSCP Mapping for WPS Sessions feature.

Note This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.

Counters	Description
dpca-imsa-total-session-priority-channel	Shows the cumulative number of Wireless Priority subscribers.
dpca-imsa-total-sessions-switched-from-priority-channel	Shows the cumulative number of subscribers moved from Wireless Priority to Normal.
dpca-imsa-total-sessions-switched-to-priority-channel	Shows the cumulative number of subscribers moved from Normal to Wireless Priority.

P-GW Schema

The following bulk statistics are added in the epdg-plmn-schema to support Bulk Statistics Variables for the APN, QCI, and ARP-based DSCP Mapping for WPS Sessions feature.

Note This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.

Counters	Description
sessstat-pdn-wps-cumulative-activated	Shows the total number of P-GW PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
sessstat-pdn-wps-cumulative-deactivated	The total number of P-GW PDNs that were either released or degrades to a non-WPS PDN.

P-GW eGTP-C S5/S8 Schema

The following bulk statistics are added to the P-GW eGTP-C S5/S8 schema in support of the APN, QCI, and ARP-based DSCP Mapping for WPS Sessions feature.

Note This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.

Counters	Description
tun-recv-cresessreq-wps	Shows the total number of tunnel create session request messages received by the system for WPS subscriber on the S5/S8 interface.
tun-sent-cresessresp-wps	Shows the total number of tunnel create session response messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-recv-modbearerreq-wps	Shows the total number of tunnel modify bearer request messages received by the system for WPS subscriber on the S5/S8 interface.
tun-sent-modbearerresp-wps	Shows the total number of tunnel modify bearer response messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-sent-crebearerreq-wps	Shows the total number of tunnel create bearer request messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-recv-crebearerresp-wps	Shows the total number of tunnel create bearer response messages received by the system for WPS subscriber on the S5/S8 interface
tun-sent-updbearerreq-wps	Shows the total number of tunnel update bearer request messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-recv-updbearerresp-wps	Shows the total number of tunnel update bearer response messages received by the system for WPS subscriber on the S5/S8 interface.

SAEGW Schema

The following bulk statistics are added in the SAEGW schema to support the APN, QCI, and ARP-based DSCP Mapping for WPS Sessions feature.

Note This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.

Counters	Description
pgw-anchor-pdns-wps-cumulative-activated	Shows the total number of P-GW anchored PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
pgw-anchor-pdns-wps-cumulative-deactivated	Shows the total number of P-GW anchored PDNs that were either released or degrades to a non-WPS PDNs.
saegw-colocated-pdns-wps-cumulative-activated	Shows the total number of SAE-GW collapsed PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
saegw-colocated-pdns-wps-cumulative-deactivated	Shows the total number of SAE-GW collapsed PDNs that were either released or degrades to a non-WPS PDN.
sgw-anchor-pdns-wps-cumulative-activated	Shows the total number of S-GW anchored PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
sgw-anchor-pdns-wps-cumulative-deactivated	Shows the total number of S-GW anchored PDNs that were either released or degrades to a non-WPS PDN.

S-GW Schema

The following bulk statistics are included in the S-GW Schema to support the APN, QCI, and ARP-based DSCP Mapping for WPS Sessions feature.

Note This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.

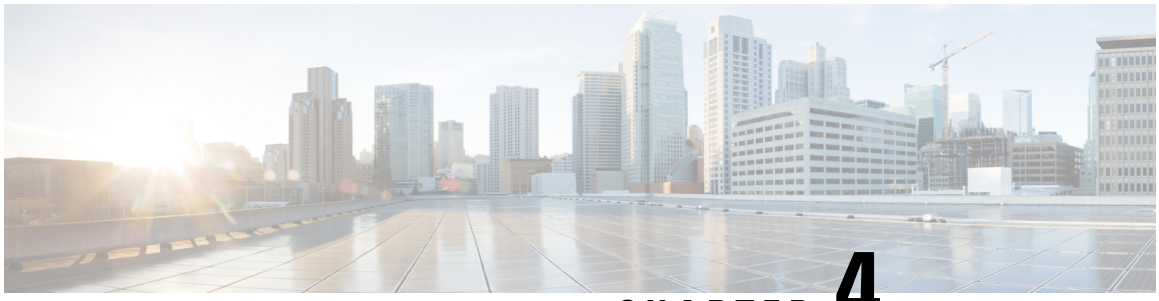
Counters	Description
sessstat-pdn-wps-cumulative-activated	Shows the total number of S-GW PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
sessstat-pdn-wps-cumulative-deactivated	The total number of S-GW PDNs that were either released or degrades to a non-WPS PDN.

Deprecated Bulk Statistics

None in this release.

Modified Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.23

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.23 software release.

SNMP MIB Alarm Changes for 21.23

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

SNMP MIB Conformance Changes for 21.23

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

SNMP MIB Object Changes for 21.23

This section provides information on SNMP MIB alarm changes in release 21.23.

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 21.23.

- starSRPPeerVersion
- starSXPeerVersion
- starChassisState
- starSxPeerUnsupportedVersion

- starSxPeerUnsupportedVersionClear
- starSRPPeerUnsupportedVersion
- starSRPPeerUnsupportedVersionClear

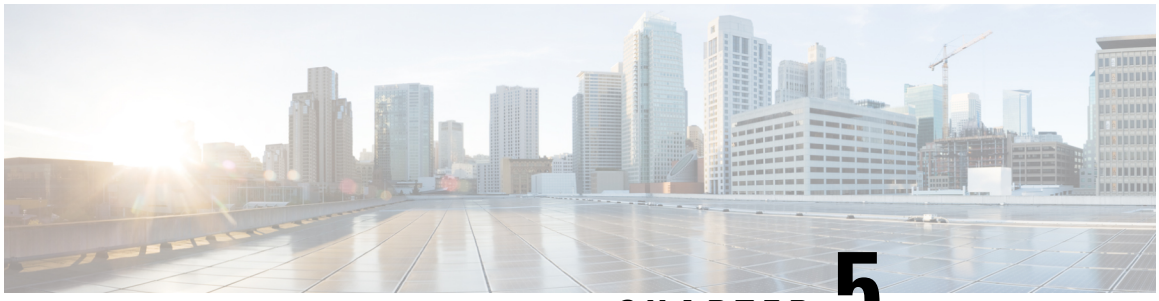
Modified SNMP MIB Object

- starThreshPerServicePDSNSessions
- starThreshClearPerServicePDSNSessions
- starThreshPerServiceGGSNSessions
- starThreshClearPerServiceGGSNSessions
- starThreshPerServiceHASessions
- starThreshClearPerServiceHASessions
- starThreshPerServiceLNSSessions
- starThreshClearPerServiceLNSSessions
- starThreshClearCDRFlowControl
- starThreshClearPerServiceSGSNSessions
- starThreshPerServiceSGSNPdpSessions
- starThreshClearPerServiceSGSNPdpSessions
- starThreshPerServiceASNGWSessions
- starThreshClearPerServiceASNGWSessions
- starThreshPerServiceGPRSSessions
- starThreshClearPerServiceGPRSSessions
- starThreshPerServiceGPRSPdpSessions
- starThreshClearPerServiceGPRSPdpSessions
- starThreshCSCFSvcErrorNoResource
- starThreshPerServicePCCPolicySessions
- starThreshClearPerServicePCCPolicySessions
- starThreshPerServicePCCQuotaSessions
- starThreshClearPerServicePCCQuotaSessions
- starThreshPerServicePCCAFSessions
- starThreshClearPerServicePCCAFSessions
- starThreshClearPerServicePDGSessions
- starThreshPerServiceSAMOGSessions

- starThreshClearPerServiceSAMOGSessions
- starCdrPurged
- starTechSuppPasswdChanged
- starMonSubProcessInitFailure
- starUPlaneTsServiceChainPathNotSelected
- starUPlaneTsServiceChainUp
- starUPlaneTsServiceChainDown
- starUPlaneTsMissConfiguration

Deprecated SNMP MIB Object

None in this release.



CHAPTER 5

4G Network Upgrade on Gx Interface

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.23

Feature Description

Diameter Overload Indication Conveyance (DOIC) specification passes overload information during transfer of messages to P-GW server. When there is an overload, there is no specific way to choose the messages that needs to be throttled or discarded which could result in excess traffic in the network. To reduce traffic in the network, Diameter Routing Message Priority (DRMP) is newly introduced. Using DRMP, you can set the priority for messages, based on which messages are throttled or discarded.

DRMP messages can be sent in CCR message and RAA in Gx interface only. The value to be sent in AVP can be configured using the configuration commands for below messages:

Message	Description
CCR -Initial	The CCR message is sent during connection creation.
CCR- Update	The CCR message that is sent during CCR update.
CCR-Termination	The CCR message that is sent during connection deletion.
RAA	ReAuth Answer message that is sent in response to the ReAuth Request from the PCRF.

Note If the DRMP feature is not configured, then no priority is set in the CCR/RAA messages. If DRMP is set without any priority (0 to 15), then the default priority of 10 will be set.

Configuring DRMP Priority Values

Use the following configuration commands to set the priority DRMP value:

```
configure
    context context_name
      ims-auth-service ims_auth_service_name
        policy-control
          [ no ]diameter{ drmp [ ccr-i drmp_value| ccr-t drmp_value| ccr-u
drmp_value |rra  drmp_value]}
  end
```

Note If the DRMP feature is not configured, then no priority is set in the CCR/RAA messages. If DRMP is set without any priority (0 to 15), then the default priority of 10 will be set.

Origination Time Stamp and Maximum Wait Time

Origination-Time-Stamp

Origination-Time-Stamp(1536) is a standard AVP that is added in the CCR-I messages originating from P-GW. This AVP indicates the time (NTP synced) when the request message is sent to PCRF Server from P-GW. The Origination-Time-Stamp(1536)indicates the UTC time at which the originating entity initiated the request and is encoded in the 64-bit NTP timestamp format and here, the binary encoding of the integer part is in the first 32 bits and binary encoding of the fraction part is in the last 32 bits.

Maximum-Wait-time

Maximum-Wait-time is a standard AVP (code 1537) of type of Unsigned 32. If message is received and takes a long time to process then the message is dropped by the PCRF and the CCA-I will not be sent by the PCRF. This AVP is used along with origination-timestamp AVP. Max-Wait-time (7103) is the non-standard AVP used in CCR-I messages towards Diameter Gx and it is used along with the Maximum-Wait-Time (1537) standard AVP.

Table 1: Existing AVP's

AVP Name	AVP ID
Origination-Timestamp	7102
Max-Wait-Time	7103

Table 2: New AVP's

AVP Name	AVP ID
Origination-Time-Stamp	1536
Maximum-Wait-Time	1537

Note Both new and existing AVPs are supported in this release.

Monitoring and Trouble Shooting

This section provides information on the show commands and bulk statistics.

Show Command and Output

show ims-authorization service name <service_name>

The following new fields are added to the output of this command:

- Diameter Policy Control
  - DRMP: CCR-I CCR-U CCR-T RAA

show ims-authorization policy-control statistics

The following new fields are added to the output of this command:

- DPCA Experimental Result Code Stats
  - Late Overlapping Request
  - Time Out Request

show session disconnect-reasons

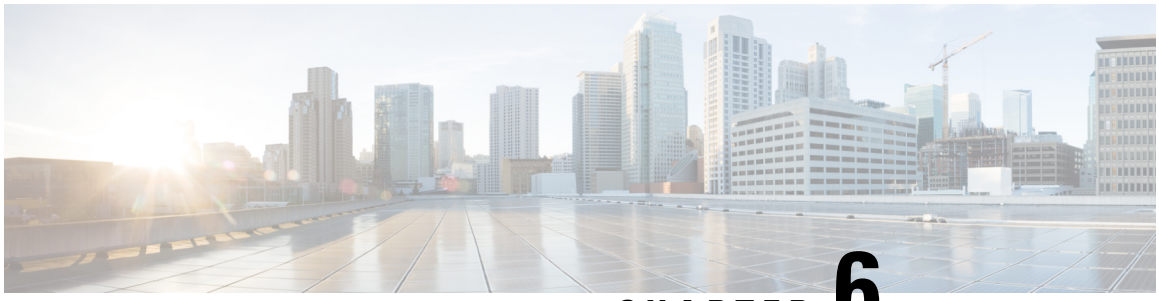
The following new fields are added to the output of this command:

- Disconnect Reason
  - newer-session-detected
  - late-overlapping-request

Bulk Statistics

The following bulk statistics are newly added:

Bulk Statistics	Description
dpca-imsa-exp-late-overlapping-request	Displays the total number of times the diameter experimental result code DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST(5453) is received in CCA message.
dpca-imsa-exp-timed-out-request	Displays the total number of times the diameter experimental result code DIAMETER_ERROR_TIME_OUT_REQUEST(5454) is received in CCA message.



CHAPTER 6

APN, QCI, and ARP-based DSCP Mapping for WPS Sessions

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	Not applicable

Revision History

Revision Details	Release
First introduced. **Important** This feature is not validated for all customer deployment scenarios. For more information, contact your Cisco Account representative.	21.23

Feature Description

The APN, QCI and ARP-based DSCP Mapping for WPS Sessions feature enables P-GW and S-GW to support DSCP marking based on APN, QCI and ARP functionality for Wireless Priority Service subscribers.

Prioritization of Control Plane Traffic: WPS user's control plane traffic is prioritized over other subscribers between different Network Functions in the LTE Core.

Priority Levels: P1, P2, and P3 are the three priority levels available for WPS users:

- P1 and P2 users are identified in HSS/PCRF and GW uses their priority (APN, QCI, and ARP) during default and dedicated bearer creation, modification, update, or deletion.
- P1 and P2 WPS users are always treated as High Priority.
- DSCP markings for prioritized user's control plane IP packets is marked with DSCP=47 while all other users control packets IP packets is marked with DSCP=32.
- Non-WPS users and P3 WPS users (for example, with QCI=5 and ARP PL =5) are given high priority dynamically based on a call being placed. Example: WPS-P1 user calling non-WPS user.
- For the LTE Core, the indication of higher priority for a user comes over Rx based on the presence of MPS-Identifier-AVP and value of Service-Info-Status-AVP in the Rx-AAR. PCRF takes appropriate actions and then propagates appropriate QCI, ARP values over to P-GW on Gx session.

Diameter Interfaces:

- P-GW, Policy Change Rule Function (PCRF), and Diameter Routing Agent (DRA) uses the configuration of Diameter interfaces such as Gx and Rx interfaces to support policy and charging control for subscribers.

Non-Diameter Interfaces: P-GW and S-GW uses non-diameter interfaces such as S5, S8, S11, or S1U with its peer respectively.

Characteristics of Low and High Priority Channels for Diameter based Interfaces

Low Priority channels are used for non-WPS user sessions and High Priority channels are used for WPS user sessions. These channels are identified by different Differentiated Services Code Point (DSCP) markings. The peer connections towards DRA for PGW (Gx) isshown in the figure.

Figure 1: High-Level Overview of Low and High Priority Channels over Gx Interface

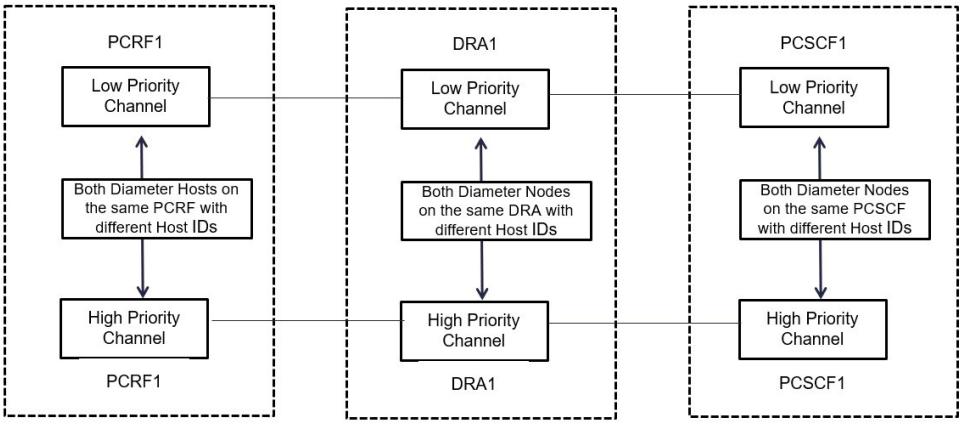


Table 3: Low and High Priority Channels on Gx Interface

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	Gx	Equal to 32	32 **Note** This channel is for non-WPS diameter messages but may carry WPS diameter messages in error scenarios, for example when all the Red Peers are down.	Not Modified Examples: 0 0 0 1-diamproxy. PGW-Gx', 'dra1', 'pcrf1
High Priority	Gx	Equal to 47	47	Specific to High Priority Examples: 0001-diamproxy. PGW-Gx-wps', ' dra1-wps', 'pcrf1-wps'.

Characteristics of Low Priority and High Priority Channels for S11, S5, or S8 interfaces

The S5 and S11 interfaces are GTPv2 based (which uses UDP as the transport protocol), Low and High Priority channels have the following characteristics.

Table 4: Low and High Priority Channels on Other Interfaces

Priority Channel	Diameter Interfaces	IP Layer DSCP	TCP Connection over IP layer	Diameter Host FQDN
Low Priority	S11 or S5 or S8	32	—	—
High Priority	S11 or S5 or S8	47	—	—

How it Works

The following is a high-level overview of how this feature works.

The P-GW/S-GW selects either High Priority or Low Priority channels based on the wps profile. The following table describes the DSCP marking rules based on the configured APN name, QCI values, and ARP PL in the default or any of the dedicated bearer of a session. WPS session detection is based on the configured APN name, QCI and ARP PL values in the default or dedicated bearer of a session. The S5, S8 and S11 interface contain IP packets marked with DSCP=47 IP based on APN, QCI, and ARP PL parameters as shown in the table. Other IP packets are marked with DSCP=32.

Table 5: WPS Message Prioritization based on APN, QCI, and ARP Priority Level

APN Name	QCI	ARP PL	DSCP
APN-x/APN-y/*	66,69	*	47
APN-x/APN-y/*	*	1,2	47
APN-x/APN-y/*	8	3	47
APN-x/APN-y/*	9	5	47
APN-x/APN-y/*	2	4	47

The following table explains the process of dynamic transport selection based on transaction or Origin Host:

Table 6: Procedure

Process	Description
Identifying WPS and Non-WPS users	• Use the CLI command **priority-select** at diameter end point to enable or disable WPS users. This CLI command is at policy-control configuration in IMS-authorization service. • P-GW receives Create session request with every WPS session is tagged with the APN name, QCI, and ARP PL values. • P-GW verifies whether that APN name, QCI, and ARP PL value is matching the WPS. • Session Manager checks whether the received ARP PL value matches the WPS session or not. • If the above criteria of matching WPS session and enabling of priority select is met then, the user is called as WPS user. Else, the user is called as Normal user.
Prioritizing Session	At Policy Change Rule Function (PCRF) you can define two priority levels such as Low Priority session for non-WPS users and high priority session for WPS users. • **Always-On WPS Sessions**: GTPv2-S5, GTPv2-S11, GTPv2-S8, and Gx sessions, which belongs to WPS users are always treated as high priority. • **On-Demand WPS Sessions**: GTPv2-S5, GTPv2-S11, GTPv2-S8, and Gx sessions, which belong to Non-WPS users can be uplifted to higher priority (lower ARP PL value) dynamically. The most common example of this is when a WPS user makes a WPS call (that is initiated by dialing a call starting with *272) to non-WPS user. These types of sessions are called On-Demand WPS sessions. • Control plane Gx messages belonging to high priority sessions shall use High Priority channels. • Control plane Gx messages belonging to non-high priority sessions shall use low priority channels.

Process	Description
Differentiating paths between normal users and WPS users	On Gx interface, different connections are made to form the second path at the CLI level: • P-GW creates two sets of DRA peer connections. One set for higher priority and other for normal priority messages. • P-GW sends CCR-Initial and CCR-Update Gx messages on specific pair of connections based on type of session (WPS session or non WPS session). • After the peer is configured with priority-select flag, all CCR messages for WPS session is initiated over High Priority peer. if P-GW identifies the users as a WPS user it will bind to the high priority peer with DSCP marking as 47. However, non WPS subscriber's Diameter message is initiated over Low Priority peer and the DSCP is set to 32. **Note** If the DSCP configuration for peer is not specified, then global dscp value configured under diameter endpoint is used. If global dscp value under diameter endpoint is not configured, then dscp value "0" is used. The following actions are performed before triggering CCR-I message with respect to WPS users: • Selection of High Priority peer. • If an existing AVP string is configured in peer configuration, Origin Host ID is appended with a string. If string is not configured, default **-wps** string is appended to Origin Host ID. • DRA/PCRF responds with CCA-I over high priority channel upon reception of the CCR-I. The subsequent messages follow the high priority channel.

Call Flow

The key call flow for this feature include transitioning from non-WPS to WPS Session and PCRF initiated Bearer Deletion.

If CSR (Creation Session Request) has one bearer and ARP PL, QCI does not match with ARP PL, QCI defined in WPS profile for corresponding APN, the Session is treated as Non-WPS Session. All Gx messages follow low priority channel to PCRF. However, if any dedicated bearer triggered by Mobile has ARP PL, QCI matched with ARP PL, QCI in WPS profile for corresponding APN , low priority session is transitioned to WPS session.

Note "Green peer" is "Low priority channel". "Red peer" is "High priority channel"

Figure 2: Transitioning from Non-WPS to WPS Session and Vice Versa

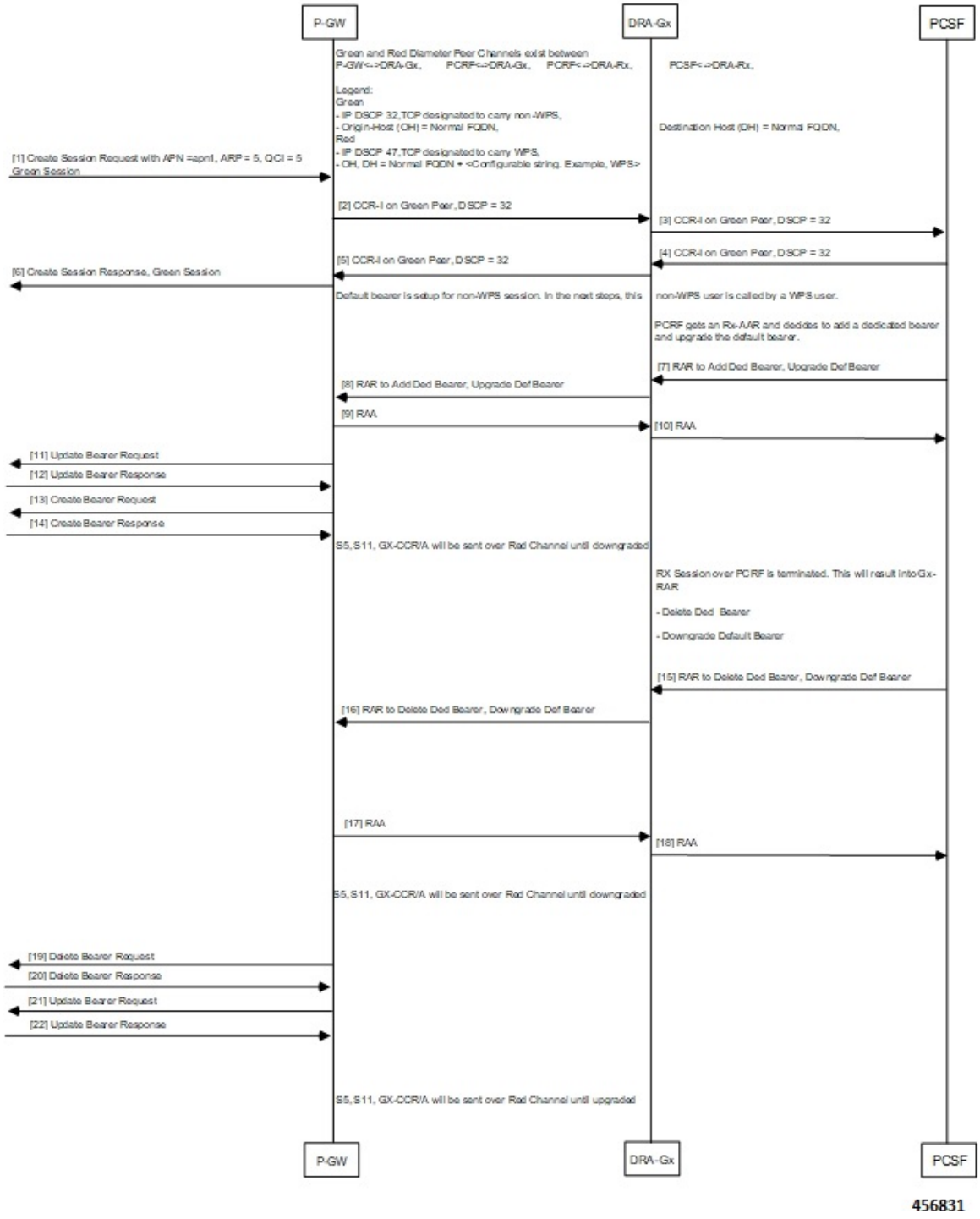


Table 7: Procedure

Step	Description
1 through 6	Low Priority channels are used for a non-WPS session.
7 through 14	P-GW receives dedicated bearer with APN, ARP PL, QCI matched with ARP PL in WPS APN profile, the following operations are performed, and CCR-U is sent to DRA/PCRF. • Non-WPS session is transitioned to WPS session. CLP is updated as WPS session. • P-GW Identifies high priority peer. • Appends the String "-wps" or configured origin-host-suffix string to Origin host ID. The subsequent outgoing messages on Gx, S5, S11, or S8 will follow the high priority channel until the session is downgraded again.
15 through 22	P-GW receives RAR with QCI or ARP PL that are not defined in WPS APN profile, the session is downgraded from WPS session to non-WPS.

Configuring IMS Authorization Service for WPS

Use the following sample configuration to configure IMSA service at context level for IMS subscribers:

```
configure
   context context_name
      ims-auth-service imsa_service_name
         policy-control
            diameter origin endpoint endpoint_name priority-select
            diameter dictionary dictionary
            no event-report-indication
            custom-reauth-trigger  qos-change default-bearer-qos-change
ue-ip-addr-allocate resource-modification-request  ue-ip-addr-release
apn-ambr-mod-failure default-bearer-qos-mod-failure
            diameter host-select table { 1 | 2 } algorithm round-robin
            diameter host-select row-precedence  precedence_value  table { 1 |
 2 } host  primary_host_name  [ realm  primary_realm_id  ] [ secondary host
secondary_host_name  [ realm  secondary_realm_id  ] ] priority-host [ -noconfirm
]
            exit
         exit
```

NOTES:

- *context_name* must be the name of the context where you want to enable IMSA service.
- *imsa_service_name* must be the name of the IMSA service to be configured for Rel. 8 Gx interface authentication.

- To enable Rel. 8 Gx interface support, pertinent Diameter dictionary must be configured. For information on the specific Diameter dictionary to use, contact your Cisco account representative.
- The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
- **priority-select**: Enables Wireless Priority Services (WPS) for subscribers. This is a mandatory parameter to define peer as Red peer.

Note **priority-select** keyword is used under IMSA as well as under 'diameter endpoint' configuration. Both must be enabled for current feature to work.

- **priority-host**: Configures host as red host. If priority-host keyword configured in a row, both primary and secondary peers are treated as red host .

Note To remove this keyword, configure **no-priority-host**.

Configuring DSCP Mapping

This section describes how to configure the DSCP mapping:

- Configuring a WPS APN Profile.
- Associating an WPS profile with P-GW and S-GW service
- Enabling Gx Prioritization for WPS Sessions
- Differentiating Low Priority and High Priority Peers

Configuring WPS APN Profile

Use the following commands to configure WPS APN profile, which is used to identify a bearer or session as an WPS bearer or session.

```
configure
     wps-apn-profile  wps_apn_name
     [ no ] wps-apn-row row_number qci qci_value earp arp_pl_value dscp dscp_value
end
```

NOTES:

- **wps-apn-profile** *wps_apn_name*: Configures WPS profile for an APN. This APN name is used for wps session detection. **wps-apn-profile all** is used when this WPS APN Profile is to be applied for all APNs.

Important Different **wps-apn-profile** must be defined for different APNs.

- **wps-apn-row**: This configuration is used for marking a bearer/PDN as an WPS. QCI and eARP PL are used for wps session detection. You can configure maximum of 16 rows and an integer value from 1 to16.

  For the **qci and earp**, **all** is the wild card match.

- **dscp**: This configuration is used at S-GW or P-GW, to mark various outgoing GTP-C and Gx messages associated with an WPS PDN with configured DSCP marking. The dscp value is an integer between 1..63.

Associating WPS APN Profiles with P-GW and S-GW Services

This section describes how to associate a WPS APN profile with P-GW and S-GW services.

```
configure
   context  context_name
      [ no ] pgw-service service_name
         [ no ] associate wps-apn
         end
```

Notes:

- **no**: Disables WPS APN profile association with P-GW service.
- **associate wps-apn**: Associates WPS APN profile with P-GW service.

```
configure
   context context_name
      [ no ] sgw-service  service_name
         [ no ] associate wps-apn
         end
```

Notes:

- **no**: Disables WPS APN profile association with S-GW service.
- **associate wps-apn**: Associates WPS APN profile with S-GW service.

Enabling Gx Prioritization for WPS Sessions

This section describes how to enable Gx prioritization levels for WPS sessions

```
configure
   context context_name
      [ no ]ims-auth-service service_name
         [ no ] policy control
             [ no ] diameter origin endpoint  endpoint_name  priority-select
             [ no ] diameter session-prioritization
            diameter host-select row-precedence precedence_value table { 1 |
2 } host primary_host_name [ realm primary_realm_id ] [ secondary host
secondary_host_name [ realm secondary_realm_id  ] ]  priority-host [ -noconfirm
]
         end
```

Notes:

- **priority-select**: Enables Wireless Priority Services (WPS) for the selected IMS authorization service.

  Note The **priority-select** keyword is mandatory for WPS feature.

- **no diameter session-prioritization**: Enables or disables Gx signalling prioritization for WPS sessions:
  - By default, the **diameter session-prioritization** CLI command is disabled and Gx messages does not get prioritized based on WPS value.
  - If previously configured, use the **no diameter session-prioritization** CLI command to set the default behavior
  - The **diameter session-prioritization** CLI takes effect when Gx, along with WPS APN profile, is enabled in the configuration.
  - The **diameter session-prioritization**configuration attaches DRMP-0 AVP to Diameter Messages going over the High Priority channel. DRA/PCRF takes appropriate actions based on DRMP-0, incase of fallback from High Priority to Low Priority channel takes place on P-GW to DRA or DRA to PCRF Gx links.

    Note Diameter session-prioritization is an existing CLI and it is not mandatory for configuring WPS feature.

  - **priority-host**: Configures host as red host. If priority-host keyword configured in a row, both primary and secondary peers are treated as red host.

Differentiating Low Priority and High Priority Peers

This section describes how to differentiate between low and priority peers. Priority-endpoint configuration under policy-control ensures WPS feature is only applicable to IMS auth service under policy control area. It is applicable for Gx interface

```
configure
   context context_name
      [ no ] diameter endpoint pgw-gx
        peer  primary_peer_name [ realm primary_realm_name ] address ip_address [
port port_number ]
         peer  secondary_peer_name [ realm secondary_realm_name ] address ip_address
 [ port port_number ] priority-select dscp dscp_value origin-host-suffix
suffix_name
          end
```

NOTES:

- **priority-select**: Defines peer as high priority wps peer. It is optional to configure to both parameters. Following conditions apply during peer configuration:
  - If **priority-select** is not configured, peer will not be treated as high priority **WPS** peer.

- If no DSCP at peer is configured, endpoint level DSCP is filled in IP packets towards DRA/PCRF. Otherwise, configured DSCP is filled in IP packet.
- If Priority-select is set and **origin-host-suffix** is configured in peer, configured string is added to Origin Host ID. Otherwise, default "-wps" string is added to origin host id (for example, pgw-gx-wps).
- **dscp**: DSCP can also be configured on low priority peer. The dscp value is a integer between 1..63.

Monitoring and Troubleshooting

This section describes troubleshooting information, show commands and Outputs, IMSA level statistics, eGTPC statistics, and Bulk statistics.

Show Commands and Outputs

show ims-authorization policy-control statistics

Use this CLI command to view the output field details of `Rule Installation Failure` statistics, number of prioritized DRMP messages, WPS and Non-WPS session statistics

Field	Description
DPCA WPS Session Stats	
Total Current Sessions	The total number of DPCA WPS session currently running on this system
Switched from Priority Chnl	Indicates the total subscribers moved from Wireless Priority to Normal
Switched to Priority Chnl	Indicates the total subscribers moved from Normal to Wireless Priority
DPCA WPS Message Stats	
Priority Channel Indicates message statistics for WPS session, which is sent or received on high priority channel.	
Total messages Received	Total policy control messages received for IMS authorization policy control.
Total Messages Sent	Total messages sent to IMS authorization policy control server.
Total CCR	Total Credit Control Request (CCR) messages received.
Total CCA	Total Credit Control Answer (CCA) messages sent in response to CCRs.
CCR-Initial	Total number of initial CCR messages received.
CCA-Initial	Total number of initial CCA messages sent in response to initial CCR messages.

Field	Description
CCA-Initial Accept	Total number of initial CCA messages accepted in response to initial CCR messages.
CCA-Initial Reject	Total number of initial CCA messages rejected in response to initial CCR messages.
CCA-Initial Dropped	Total number of CCA-I messages that are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode.
CCA-Initial Timeouts	Total number of initial CCA messages timed out in response to initial CCR messages.
CCR-Update	Total number of Credit Control Request (CCR) messages received after initial CCR for update.
CCA-Update	Total Credit Control Answer (CCA) messages sent in response to update CCRs.
CCA-Update Timeouts	Total Credit Control Answer (CCA) messages sent in response to update CCRs but timed out.
CCA-Update Errors	Total number of errors in parsing the CCA-Update Message.
CCA-Update Dropped	Total number of CCA-U messages that are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode.
CCR-Final	Total number of final CCR messages received to end application.
CCA-Final	Total number of final CCA messages sent in response to final CCR messages to end sessions.
CCA-Final Timeouts	Total number of final CCA messages sent in response to final CCR messages to end sessions but timed out.
CCA-Final Errors	Total number of errors in parsing the CCA-Terminate Message.
CCA-Final Dropped	Total number of CCA-T messages, which are dropped due to S-GW restoration, DPCA is off ,or not present, or if the IMSA session is in preservation mode.
ASR	Total number of Abort-Session-Requests (ASRs) received.
ASA	Total number of Abort-Session-Accept (ASA) messages sent in response to Abort-Session-Requests (ASRs).
RAR	Total number of Re-Auth-Requests (RARs) received for re-authorization..
RAA	Total number of Re-Auth-Requests(RARs) answered with Re-Auth-Answer (RAA) message.

Field	Description
RAR-CCR collision	Total number of Re-Auth-Request (RAR) messages received from PCRF when there is any outstanding Credit Control Request (CCR) message.
Non-Priority Channel	**Indicates message statistics for WPS session, which is supposed to be sent/received on Priority channel but sent/received on Non-priority channel**
Total messages Received	Total policy control messages received for IMS authorization policy control.
Total Messages Sent	Total messages sent to IMS authorization policy control server.
Total CCR	Total Credit Control Request (CCR) messages received.
CCR-Initial	Total number of initial CCR messages received.
CCA-Initial	Total number of initial CCA messages sent in response to initial CCR messages.
CCA-Initial Accept	Total number of initial CCA messages accepted in response to initial CCR messages.
CCA-Initial Reject	Total number of initial CCA messages rejected in response to initial CCR messages.
CCA-Initial Dropped	Total number of CCA-I messages which are dropped due to S-GW restoration, DPCA is off, or not present, or if the IMSA session is in preservation mode
CCA-Initial Timeouts	Total number of initial CCA messages timed out in response to initial CCR messages.
CCR-Update	Total number of Credit Control Request (CCR) messages received after initial CCR for update.
CCA-Update	Total Credit Control Answer (CCA) messages sent in response to update CCRs.
CCA-Update Timeouts	Total Credit Control Answer (CCA) messages sent in response to update CCRs but timed out.
CCA-Update Errors	Total number of errors in parsing the CCA-Update Message
CCA-Update Dropped	Total number of CCA-U messages which are dropped due to S-GW restoration, DPCA is off or not present or if the IMSA session is in preservation mode.
CCR-Final	Total number of final CCR messages received to end application.
CCA-Final	Total number of final CCA messages sent in response to final CCR messages to end session/s..

Field	Description
CCA-Final Timeouts	Total number of final CCA messages sent in response to final CCR messages to end session/s but timed out.
CCA-Final Errors	Total number of errors in parsing the CCA-Terminate Message.
CCA-Final Dropped	Total number of CCA-T messages which are dropped due to S-GW restoration, DPCA is off or not present or if the IMSA session is in preservation mode.
ASR	Total number of Abort-Session-Requests (ASRs) received.
ASA	Total number of Abort-Session-Accept (ASA) messages sent in response to Abort-Session-Requests (ASRs).
RAR	Total number of Re-Auth-Requests (RARs) received for re-authorization.
RAA	Total number of Re-Auth-Requests (RARs) answered with Re-Auth-Answer (RAA) message.
RAR-CCR collision	Total number of Re-Auth-Request (RAR) messages received from PCRF when there is any outstanding Credit Control Request (CCR) message.

show diameter peers full all

Use this CLI command to view peer details.

Counters	Description
Priority Channel	Indicates peer is high priority or not. The options are: • Yes: Indicates peer is WPS. • No: Indicates peer is non-WPS.

show wps-apn-profile{all | name wps_apn_profile_name}

View a particular or all WPS APN profile(s) configured with its associated attributes.

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

Field	Description
WPS APN Profile(s) Associated	Indicates **wps apn profile** associated with P-GW service or not. The options are Yes and No.

You can view similar output field information for the **show sgw-service { name <name> | all }** command.

show pgw-service { name_*name* | all }

The output of this command is modified to reflect the WPS APN profile associated with the P-GW service.

Field	Description
WPS APN Profile(s) Associated	Indicates **wps apn** profile associated with pgw service or not. The options are **Yes** and **No**.

show sgw-service { name_*name* | all }

The output of this command is modified to reflect the WPS APN profile associated with the S-GW service.

Field	Description
WPS APN Profile(s) Associated	Indicates **wps apn** profile associated with sgw service or not. The options are **Yes** and **No**.

show subscribers pgw-only full all

The output of this command is modified to reflect whether the session is WPS or not.

Field	Description
WPS Bearer	Indicates whether the Bearer is a WPS or non-WPS. The options are **Yes** and **No**.

show sgw-service statistics all

The output of this command is modified to display the WPS PDN statistics information.

Field	Description
WPS PDNs	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN.

show subscribers sgw-only full all

The output of this command is modified to reflect whether the session is WPS or not

Field	Description
WPS Bearer	Indicates whether the Bearer is a WPS or non-WPS. The options are **Yes** and **No**.

show subscribers saegw-only full all

The output of this command is modified to reflect whether the session is WPS or not.

Field	Description
WPS Bearer	Indicates whether the Bearer is a WPS or non-WPS. The options are **Yes** and **No**.

show pgw-service statistics all

The output of this command is modified to display the WPS PDN statistics information.

Field	Description
WPS PDNs	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN.

show sgw-service statistics all

The output of this command is modified to display the WPS PDN statistics information.

Field	Description
WPS PDNs	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN.

show saegw-service statistics all

The output of this command is modified to display the WPS PDN statistics information.

Field	Description
WPS PDNs	

Field	Description
Colocated PDNs	Displays the WPS PDN statistics information for collapsed PDNs.
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN PGW-Anchor WPS PDNs. Displays the WPS PDN statistics information for P-GW-Anchor PDNs.
PGW-Anchor WPS PDNs: Displays the WPS PDN statistics information for PGW-Anchor PDNs.	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN PGW-Anchor WPS PDNs. Displays the WPS PDN statistics information for P-GW-Anchor PDNs.
SGW-Anchor WPS PDNs: Displays the WPS PDN statistics information for SGW-Anchor PDNs.	
Current Active	Increments when any PDN is setup as an WPS PDN or upgraded to WPS PDN. Decrements when an WPS PDN is released or when it degrades to a non-WPS PDN.
Cumulative Activated	Increments when any PDN is setup as an WPS PDN or upgrades to an WPS PDN.
Cumulative De-activated	Increments when an WPS PDN is released or when it degrades to a non-WPS PDN.

show egtpc statistics interface pgw-ingress interface-type S5/S8

The following CLI commands are modified to display the WPS session related GTP-C message statistics for S5/S8 interface of P-GW Ingress.

Counter	Description
Total WPS Statistics: Displays cumulative GTP-C message statistics for messages received/transmitted on WPS Sessions.	
Create Session Request (Total RX)	This counter is incremented by P-GW when it receives Create session request message on S5/S8 interface that makes session as WPS.

Counter	Description
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Create session response message on the S5/S8 interface,
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Modify Bearer request message on the S5/S8 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter will be incremented by P-GW when it transmits Modify Bearer response message on the S5/S8 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by P-GW when it receives Create Bearer request message on the S5/S8 interface..
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Create Bearer response message on the S5/S8 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Update Bearer request message on the S5/S8 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Update Bearer response message on the S5/S8 interface.
Current interval WPS Statistics: GTP-C message statistics for messages received/transmitted on WPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current WPS Statistics is displayed similarly as Total WPS Statistics.	
Create Session Request (Total RX)	This counter is incremented by P-GW when it receives Create session request message on S5/S8 interface that makes a session as WPS.
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Create session response message on the S5/S8 interface.
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Modify Bearer request message on the S5/S8 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Modify Bearer response message on the S5/S8 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by P-GW when it receives Create Bearer request message on the S5/S8 interface.
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Create Bearer response message on the S5/S8 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by P-GW when it transmits Update Bearer request message on the S5/S8 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by P-GW when it receives Update Bearer response message on the S5/S8 interface.

show egtpc statistics interface sgw-egress interface-type S5/S8

The following CLI commands are modified to display the WPS session related GTP-C message statistics for S5/S8 interface of S-GW Egress.

Counter	Description
Total WPS Statistics: Displays cumulative GTP-C message statistics for messages received/transmitted on WPS Sessions.	
Create Session Request (Total RX)	This counter is incremented by S-GW when it receives Create session request message on S5/S8 interface that makes session as WPS.
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Create session response message on the S5/S8 interface,
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Modify Bearer request message on the S5/S8 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter will be incremented by S-GW when it transmits Modify Bearer response message on the S5/S8 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer request message on the S5/S8 interface..
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer response message on the S5/S8 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Update Bearer request message on the S5/S8 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Update Bearer response message on the S5/S8 interface.
Current interval WPS Statistics: GTP-C message statistics for messages received/transmitted on WPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current WPS Statistics is displayed similarly as Total WPS Statistics.	
Create Session Request (Total RX)	This counter is incremented by S-GW when it receives Create session request message on S5/S8 interface that makes a session as WPS.
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Create session response message on the S5/S8 interface.
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Modify Bearer request message on the S5/S8 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Modify Bearer response message on the S5/S8 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer request message on the S5/S8 interface.

Counter	Description
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer response message on the S5/S8 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Update Bearer request message on the S5/S8 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Update Bearer response message on the S5/S8 interface.

show egtpc statistics interface sgw-ingress interface-type s11

The following CLI commands are modified to display the WPS session related GTP-C message statistics for S11 interface of S-GW Ingress

Counter	Description
Total WPS Statistics: Displays cumulative GTP-C message statistics for messages received/transmitted on WPS Sessions.	
Create Session Request (Total RX)	This counter is incremented by S-GW when it receives Create session request message on the S11 interface that makes session as WPS.
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Create session response message on the S11 interface,
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Modify Bearer request message on the S11 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter will be incremented by S-GW when it transmits Modify Bearer response message on the S11 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer request message on the S11 interface..
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer response message on the S11 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Update Bearer request message on the S11 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Update Bearer response message on the S11 interface.
Current interval WPS Statistics: GTP-C message statistics for messages received/transmitted on WPS Sessions for current statistics collection interval. Statistics collection interval will be same as bulkstats collection interval. If bulk stats collection is not configured, then Current WPS Statistics is displayed similarly as Total WPS Statistics.	
Create Session Request (Total RX)	This counter is incremented by S-GW when it receives Create session request message on S11 interface that makes a session as WPS.

Counter	Description
Create Session Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Create session response message on the S11 interface.
Modify Bearer Request (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Modify Bearer request message on the S11 interface.
Modify Bearer Response (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Modify Bearer response message on the S11 interface.
Create Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer request message on the S11 interface.
Create Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Create Bearer response message on the S11 interface.
Update Bearer Request (Total TX)	If a session is WPS, this counter is incremented by S-GW when it transmits Update Bearer request message on the S11 interface.
Update Bearer Response (Total RX)	If a session is WPS, this counter is incremented by S-GW when it receives Update Bearer response message on the S11 interface.

clear egtpc

The following CLI commands are modified to clear WPS statistics at interface level and eGTP-C service level:

- **clear egtpc statistics interface-type interface-pgw-ingress interface s5s8**: Clears interface statistics along with WPS statistics for all eGTP-C services of P-GW Ingress type and S5/S8 interface.
- **clear egtpc statistics interface-type [interface-sgw-ingress | interface-sgw-egress] interface [s11 | sgw-s5s8]** : Clears interface statistics along with WPS statistics for all eGTP-C services of S-GW Ingress type and S11 interface/S-GW Egress type and S5/S8 interface.
- **clear egtpc statistics egtp-service pgw_egtpc_service_name interface [s5s8]** : Clears interface statistics along with WPS statistics for all P-GW eGTP-C services and S5/S8 interface.
- **clear egtpc statistics egtp-service sgw_egptc_service_name interface [s11 | sgw-s5s8]** : Clears interface statistics along with WPS statistics for all S-GW eGTP-C services and S11 or S5/S8 interface.

Bulk Statistics

This section provides information on the bulk statistics in support of the QCI and ARP based DSCP mapping feature.

IMSA Schema

The following bulk statistics are included in the IMSA Schema to track high and low priority categories for WPS and Non-WPS users.

Counters	Description
dpca-imsa-total-session-priority-channel	Shows the cumulative number of Wireless Priority subscribers.
dpca-imsa-total-sessions-switched-from-priority-channel	Shows the cumulative number of subscribers moved from Wireless Priority to Normal.
dpca-imsa-total-sessions-switched-to-priority-channel	Shows the cumulative number of subscribers moved from Normal to Wireless Priority.

PGW Schema

The following bulk statistics are included in the P-GW Schema.

Counters	Description
sessstat-pdn-wps-cumulative-activated	Shows the total number of P-GW PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
sessstat-pdn-wps-cumulative-deactivated	The total number of P-GW PDNs that were either released or degrades to a non-WPS PDN.

SGW Schema

The following bulk statistics are included in the S-GW Schema.

Counters	Description
sessstat-pdn-wps-cumulative-activated	Shows the total number of S-GW PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
sessstat-pdn-wps-cumulative-deactivated	The total number of S-GW PDNs that were either released or degrades to a non-WPS PDN.

SAEGW Schema

The following bulk statistics are added in the SAEGW schema to support Bulk Statistics Variables.

Counters	Description
pgw-anchor-pdns-wps-cumulative-activated	Shows the total number of P-GW anchored PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
pgw-anchor-pdns-wps-cumulative-deactivated	Shows the total number of P-GW anchored PDNs that were either released or degrades to a non-WPS PDNs.
saegw-colocated-pdns-wps-cumulative-activated	Shows the total number of SAE-GW collapsed PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
saegw-colocated-pdns-wps-cumulative-deactivated	Shows the total number of SAE-GW collapsed PDNs that were either released or degrades to a non-WPS PDN.

Counters	Description
sgw-anchor-pdns-wps-cumulative-activated	Shows the total number of S-GW anchored PDNs that are either setup as an WPS PDN or upgrades to an WPS PDN.
sgw-anchor-pdns-wps-cumulative-deactivated	Shows the total number of S-GW anchored PDNs that were either released or degrades to a non-WPS PDN.

eGTP-C Schema

The following new bulk statistics variables are added to the eGTP-C schema in support of this feature. These statistics are only for the current bulkstat intervals.

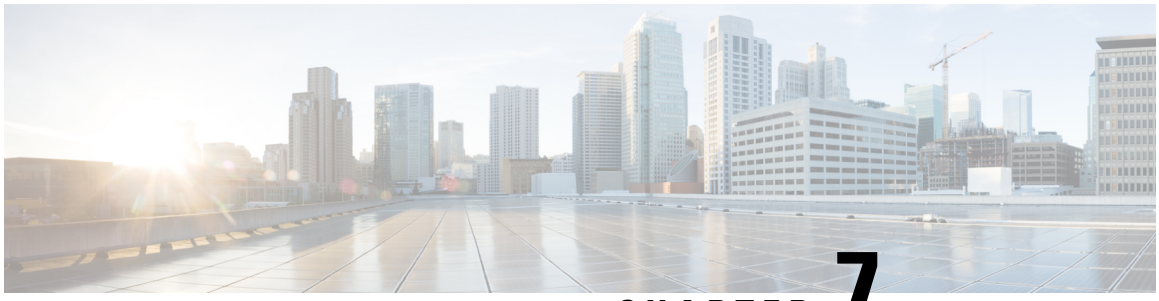
Counters	Description
s11-tun-recv-modbearerreq-wps	Shows the total number of tunnel modify bearer request messages received by the system for WPS subscriber on the s11 interface.
s11-tun-sent-modbearerresp-wps	Shows the total number of tunnel modify bearer response messages sent by the system for WPS subscriber on the s11 interface.
s11-tun-sent-crebearerreq-wps	Shows the total number of tunnel create bearer request messages sent by the system for WPS subscriber on the s11 interface.
s11-tun-recv-crebearerresp-wps	Shows the total number of tunnel create bearer response messages received by the system for WPS subscriber on the s11 interface.
s11-tun-sent-updbearerreq-wps	Shows the total number of tunnel update bearer request messages sent by the system for WPS subscriber on the s11 interface s11.
s11-tun-recv-updbearerresp-wps	Shows the total number of tunnel update bearer response messages received by the system for WPS subscriber on the s11 interface .
tun-sent-cresessreq-wps	Shows the total number of tunnel create session request messages sent by the system for WPS subscriber on the s5/s8 interface .
tun-recv-updbearerresp-wps	Shows the total number of tunnel update bearer response messages received by the system for WPS subscriber on the s5/s8 interface.
tun-sent-updbearerresp-wps	Shows the total number of tunnel update bearer response messages sent by the system for WPS subscriber on the s5/s8 interface .

P-GW eGTP-C S5/S8 Schema

The following bulk statistics are added to the P-GW eGTP-C S5/S8 schema in support of this feature. These statistics are only for the current bulkstat intervals.

Counters	Description
tun-recv-cresessreq-wps	Shows the total number of tunnel create session request messages received by the system for WPS subscriber on the S5/S8 interface.

Counters	Description
tun-sent-cresessresp-wps	Shows the total number of tunnel create session response messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-recv-modbearerreq-wps	Shows the total number of tunnel modify bearer request messages received by the system for WPS subscriber on the S5/S8 interface.
tun-sent-modbearerresp-wps	Shows the total number of tunnel modify bearer response messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-sent-crebearerreq-wps	Shows the total number of tunnel create bearer request messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-recv-crebearerresp-wps	Shows the total number of tunnel create bearer response messages received by the system for WPS subscriber on the S5/S8 interface
tun-sent-updbearerreq-wps	Shows the total number of tunnel update bearer request messages sent by the system for WPS subscriber on the S5/S8 interface.
tun-recv-updbearerresp-wps	Shows the total number of tunnel update bearer response messages received by the system for WPS subscriber on the S5/S8 interface.



CHAPTER 7

Capability to Record and Produce Call Transactions

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
ePDG supports capability to record and produce call transactions.	21.23
First Introduced.	Release 20

Feature Description

Real Time Tool (RTT) is used in Regions and Network Operations Center (NOC) for debugging network issues and to understand user behavior. All call transactions in ePDG are generated in RTT files. The ePDG support allows to understand service impact on the ePDG chassis for WLAN offload service. ePDG transfers RTT files to the external server through SSH File Transfer Protocol (SFTP). The RTT files that are in comma separated values (.CSV) format are transferred either in compressed or non-compressed format based on the configuration to the external servers such as servers in customer network either directly or through the Cisco Collector server.

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

How it Works

This section explains about 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
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

Procedure Number	Procedure Name	Applicability
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
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

Configuring RTT for ePDG

This section provides RTT configuration information for ePDG.

Enabling RTT to Record and Produce Call Transactions

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

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

NOTES:

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

Configuring RTT

Use the following CLI commands to configure the RTT feature in ePDG.

```
configure
          context context_name
            session-event-module
              event transfer-mode push primary url URL_address
              file 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**: Specifies the external server location where the records are transferred from ePDG.
- **file name**: Specifies the RTT file name where the records are stored.
- **rotation volume**: The volume based on which the RTT file is generated.
- **rotation time**: The time based on which the RTT file is generated.

Note The RTT files are pushed to the external server based on the rotation volume or rotation time, whichever occurs first.

- **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**: Specifies the RTT file extension (.csv).
- **use-harddisk**: Specifies hard disk as the storage space for the RTT file generation.
- **remove-file-after-transfer**: Specifies RTT files to be removed after pushing the files to the external server.
- **push-interval**: Specifies the push interval time at which the RTT file are transferred from ePDG 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.

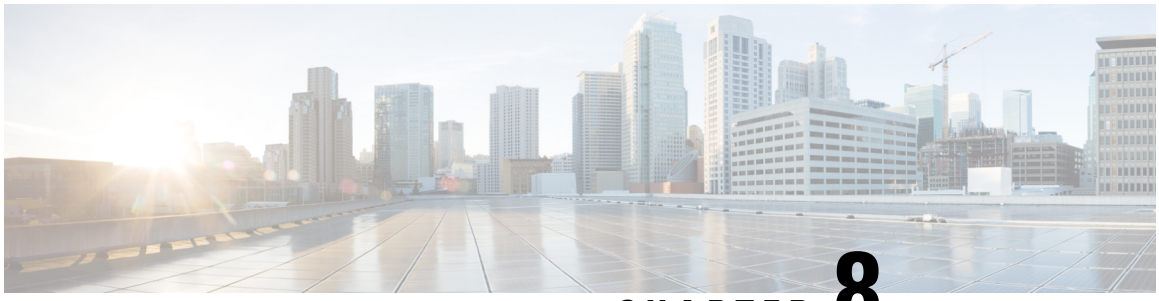
show Event-Record Statistics ePDG

This command displays the number of RTT record types generated based on different event types.

Table 8: show event-record statistics ePDG Command Output Descriptions

Field	Description
Total Number of Event Records	The total number of event records (GTPv2 + Diameter + IKE + RA).
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.
IKEv2 Event Records	The total number of IKE events.

Field	Description
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.
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.
SWm Procedures	The total number of SWm 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.



CHAPTER 8

Cisco Ultra Traffic Optimization Bulk Statistics Enhancements

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In this release, Cisco Ultra Traffic Optimization show commands and outputs are enhanced to show Rx/Tx packets statistics for Uplink and Downlink for UDP and TCP split.	21.23

Feature Description

In this StarOS 21.23 release, the following show commands and bulk statistics schema counters are enhanced to show Rx/Tx packet statistics for Uplink and Downlink for UDP and TCP split in Cisco Ultra Traffic Optimization solution.

- show active-charging traffic-optimization counters sessmgr all
- show active-charging traffic-optimization counters tcp sessmgr all
- show active-charging traffic-optimization counters udp sessmgr all

Monitoring and Troubleshooting

Show Commands and Outputs

show active-charging traffic-optimization counters sessmgr all

You can view CUTO Control Plane statistics for the following show command.

Table 9: show active-charging traffic-optimization counters sessmgr all

Field	Description
CUTO Control Plane Stats:	
Total Active Streams	Displays total number of active streams.
Active TCP Streams	Displays total number of active TCP uplink and downlink streams received.
Active UDP(QUIC) Streams	Displays total number of active UDP uplink nd downlink streams transmitted.

You can also view similar outputs for the folowing show commands:

- **show active-charging traffic-optimization counters tcp sessmgr all**
- **show active-charging traffic-optimization counters udp sessmgr all**

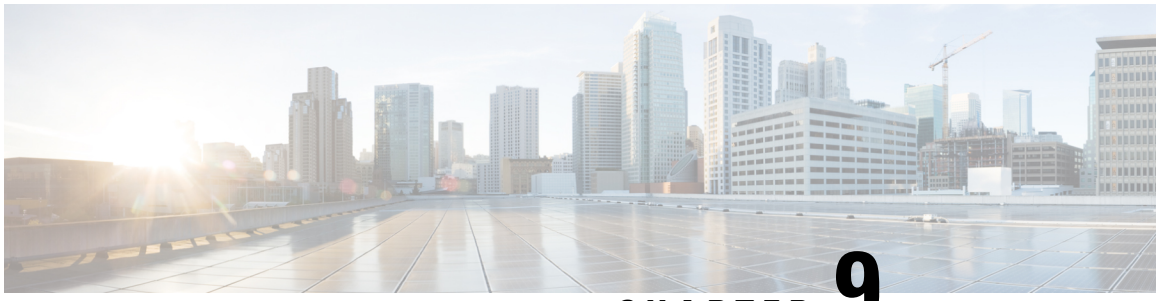
Bulk Statistics

The following bulk statistics are added in the ECS schema.

ECS Schema

Table 10: Bulk Statistics Variables in the ECS Schema

Variables	Description
cuto-tcp-uplink-rx	Indicates that the total number of TCP packets received from the UE for Cisco Ultra Traffic Optimization.
cuto-tcp-uplink-tx	Indicates that the total number of TCP packets sent towards the UE for Cisco Ultra Traffic Optimization.
cuto-tcp-dnlink-rx	Indicates that the total number of TCP packets received from the internet for Cisco Ultra Traffic Optimization.
cuto-tcp-dnlink-tx	Indicates that the total number of TCP packets sent towards the internet for Cisco Ultra Traffic Optimization.
cuto-udp-uplink-rx	Indicates that the total number of UDP packets received from the UE for Cisco Ultra Traffic Optimization.
cuto-udp-uplink-tx	Indicates that the total number of UDP packets sent towards the UE for Cisco Ultra Traffic Optimization.
cuto-udp-dnlink-rx	Indicates that the total number of UDP downlink packets received from the internet for Cisco Ultra Traffic Optimization.
cuto-dnlink-tx	Indicates that the total number of downlink packets received from the internet for Cisco Ultra Traffic Optimization.



CHAPTER 9

Closed Subscriber Group Mobility Event Support on P-GW and GGSN

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In this release, support for Closed Subscriber Groups mobility event for P-GW and GGSN is added.	21.23

Feature Description

Closed Subscriber Group (CSG) identifies a group of subscribers who are permitted to access one or more CSG cells of the Public Land Mobile Network (PLMN) as a member of the CSG. A CSG ID is a unique identifier within the scope of PLMN, which identifies a CSG in the PLMN associated with a CSG cell or group of CSG cells. For CSG information change reporting for a subscriber session requested by GGSN, the Serving GPRS Support Node (SGSN) includes the User CSG Information if the MS is located in the CSG cell or the hybrid cell.

When users enter or exit the CSG Cells or Hybrid Cells, if there are no event notifications sent back to the P-GW and Gateway GPRS Support (GGS), the capability to provide different policy and charging characteristic to the users becomes limited. In this StarOS 21.23 and later releases, CSG mobility event support is available in multiple network elements, namely eNodeB, MME, SGW, PGW, PCRF, SGSN, GGSN, HSS, and so on. This CSG mobility event feature provides full support of CSG capability on P-GW and GGSN based on 3GPP standards. This CSG mobility event feature includes capability to:

- Enable and trigger the CSG notification event.
- Apply appropriate policy and charging rules.

Access Control

The CSG Mobility Event feature functions on S5/S8, Gn/Gp, Gx, and Rf interfaces:

S5 and S8 Interfaces

The message types that processes CSG information shows the message initiated from MME and the messages initiated from PGW. S-GW passes the information from and to MME.and to and from P-GW:

- **Create Session Request**: In the Create Session Request (CSR) message, it contains a CSG Change Reporting Support Indication(CCRSI) flag when MME is configured to support CSG information change reporting to the S-GW and P-GW. If the UE is attached through a CSG or hybrid cell, the User CSG information (UCI) IE is included in the CSR. The User CSG Information IE contains the PLMN and CSG ID of the CSG or hybrid cell, the access mode (closed or hybrid), and if the access mode is hybrid, the membership status of the UE in the CSG.
- **Create Session Response**: If CSG information reporting is started or stopped, the P-GW/S-GW sends the CSG Information Reporting Action (CIRA) IE in the Create Session Response . This IE includes three bits that indicate whether the MME should report when the UE enters or leaves a CSG (non-hybrid) cell, a subscribed hybrid cell, or an unsubscribed hybrid cell. If all three bits are set to zero, all CSG information reporting to the S-GW and P-GW is stopped. The MME stores the CSG reporting information as part of the PDN context,.
- **Create Bearer Request**: If CSG reporting from the MME changes, the Create Bearer Request message from the P-GW and S-GW includes a CIRA IE. The MME stores the CSG reporting information as part of the PDN context.
- **Modify Bearer Request**: The CCRSI flag in the Indication IE is set in a Modify Bearer Request when the MME is configured to support CSG information change reporting to the S-GW and P-GW. If the

P-GW and S-GW has requested CSG information reporting and a TAU, Handover, or UE-initiated Service Request is taking place, the MME includes the UCI IE in the Modify Bearer Request message.

- **Update Bearer Request**: If CSG reporting from the MME changes, the Create Bearer Request message from the P-GW and S-GW includes a CIRA IE. The MME stores the CSG reporting information as part of the PDN context.
- **Change Notification Request**: If there is a change to the CSG connection information without a Create Bearer Request or Modify Bearer Request, the MME sends a Change Notification Request to the S-GW P-GW for each PDN where it is requested. The Change Notification Request contains a UCI IE. Since Location Reporting also uses the Change Notification Request message, the MME minimizes the number of Change Notification Request messages sent by bundling the reporting of a location change with a CSG change into the same message whenever possible.
- **Change Notification Response**: If CSG reporting from the MME changes, the Change Notification Response message from the P-GW and S-GW includes a CIRA IE. The MME stores the CSG reporting information as part of the PDN context.

Gn and Gp Interfaces

The message types that processes CSG information shows the message initiated from SGSN and the messages initiated from GGSN:

- **Create PDP Context Request (CPC Request)**: The CPC Request message contains a CSG Change Reporting Support Indication (CCRSI) flag when SGSN is configured to support CSG information change reporting to the GGSN. If the UE is attached through a CSG or hybrid cell, the User CSG information (UCI) IE is included in the CPC. The User CSG Information IE contains the PLMN and CSG ID of the CSG or hybrid cell, the access mode (closed or hybrid), and if the access mode is hybrid, the membership status of the UE in the CSG.

  Note Ignores UCI value on GGSN/P-GW when access mode value is reserved (2 or 3).

- **Create PDP Context Response (CPC Response)**: If CSG information reporting is to be started or stopped, the GGSN sends the CSG Information Reporting Action (CIRA) IE in the CPC Response. This IE includes three bits that indicate whether the SGSN should report when the UE enters or leaves a CSG (non-hybrid) cell, a subscribed hybrid cell, or an unsubscribed hybrid cell. If all three bits are set to zero, all CSG information reporting to the GGSN is stopped.
- **Update PDP Context Request (UPC Request)**: The CCRSI flag in the Extended Common Flags IE is set in UPC Request when the SGSN supports CSG Information Change Reporting and if CSG Change Reporting is requested by the GGSN through the CSG Information Reporting Action. If the UE is accessed through CSG cell or Hybrid cell, the SGSN includes the User CSG Information IE.
- .**Network Requested Update PDP Context Request (NRUPC Request)**: If CSG reporting from the SGSN changes, the NRUPC Request message from the GGSN includes a CIRA IE. The SGSN stores the CSG reporting information as part of the PDN context.
- **MS Info Change Notification Request**: The MS Info Change Notification Request contains a UCI IE and CCRSI flag in the Extended Common Flags IE. Since Location Reporting also uses the MS Info Change Notification Request message, the SGSN minimizes the number of MS Info Change Notification

Request messages sent by bundling the reporting of a location change with a CSG change into the same message whenever possible.

- **MS Info Change Notification Response**: If CSG reporting from the SGSN changes Notification Response message from the GGSN includes a CIRA IE . The SGSN stores the CSG reporting information as part of the PDN context.

Gx Interface

During CSG handling related messages over Gx interface the following functions happen:

- **Internet Protocol**: During an Internet Protocol connectivity Access Network (IP-CAN) session, the PCRF determines whether the reports for change of CSG cell or Hybrid cell is required for an IP-CAN session.
- When the UE enters or leaves the CSG or Hybrid cell, Policy and Charging Enforcement Function (PCEF) reports either USER_CSG_INFORMATION_CHANGE, USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE, or USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE event. PCEF also reports the CSG change within the User-CSG-Information AVP.
- If CSG-Information-Reporting AVP is not received in subsequent CCA-U messages, existing CSG-Information-Reporting values are reused.
- CSG-Information-Reporting AVP is used by PCRF to inform PCEF to report the user CSG information change to the Charging Data Function (CDF)/ Offline Charging Server (OFCS) over RF interface. If this AVP is not received during IPCAN session, PCEF does not report the user CSG information change to the CDF/OFCS.

Rf Interface

The ACR messages in the CSG information handling involve:

- User CSG Information (UCI) at PS level (Ps-Information AVP) to send information only during ACR start message. Sends UCI information SDC level (Service-Data-Container AVP) in subsequent messages

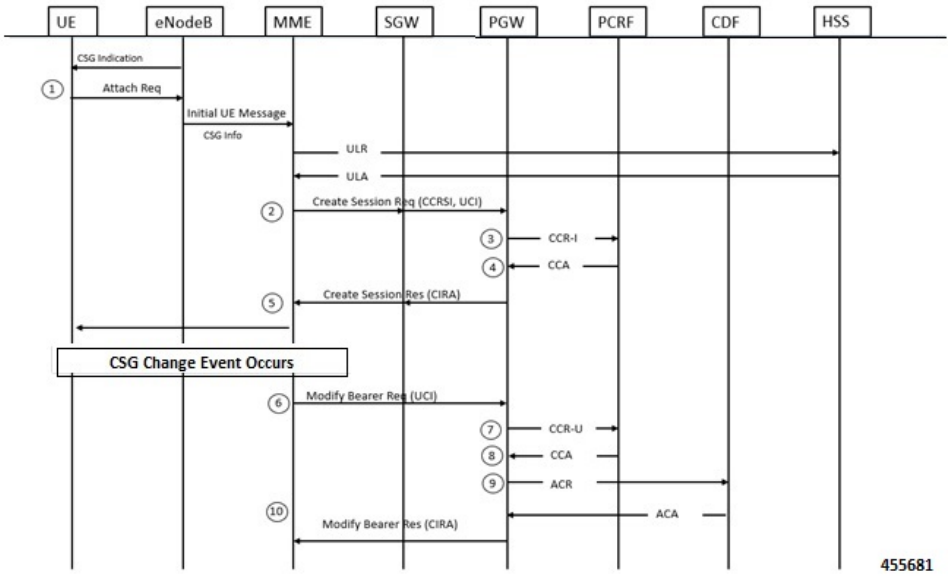
Important Configuration **attribute csg** in the Rf profile enables UCI information at PS level when transmitted in the ACR start message.

- User CSG Information (UCI) change value gets added in the Change-Condition AVP at SDC level every time when change of User CSG Information is received from access side and CSG change reporting to OFCS in CSG Information is enabled in the Reporting AVP from PCRF.
- If CSG Information Reporting is not received during IP-CAN session, P-GW does not send User CSG Information AVP to OFCS over Rf interface.

How it Works

The following diagram shows the messaging between the EPC elements in a Closed Subscriber Group implementation.

Figure 3: Closed Subscriber Groups Message Call Flow



The following steps describes the workflow:

1. The eNodeB broadcasts the CSG Information to UEs. When an Attach Request event happens, the eNodeB sends its own CSG-related Information in Initial UE message to the MME. The MME sends an Update Location Request (ULR) to the HSS to get subscriber's profile. The HSS responds with an update Location Answer including subscription-data which includes CSG-subscription-data.
2. The MME proceeds with the call according to the user profile from the HSS. The MME sets the CSG membership Indication and passes it to the S-GW including Access Mode and CSG-ID. The S-GW transparently passes the information to the P-GW.
3. The P-GW requests policy and charging rule from the PCRF.
4. The PCRF sends Event-Trigger:=USER_CSG_INFORMATION_CHANGE, USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE and USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE and CSG-Information-Reporting AVP based on the user subscription profile.
5. The P-GW sets CSG-Information-Reporting-Action in Create Session Response when the P-GW receives Event-Trigger:=USER_CSG_INFO_CHG.
6. The MME sends CSG-Membership-Status to eNodeB. This is only occurs when the Access mode is set to Hybrid.
7. The eNodeB/MME reports the event when a CSG change event happens. The MME updates CSG change event using a Change Notification Request or Modify Bearer Request.

8. The P-GW reports CSG change event using Event-Reporting-Indication AVP to the PCRF.
9. The PCRF updates the policy and charging rule with Charging-Rule-Base-Name or install new Charging-Rule-Base-Name.
10. The P-GW reports charging record to CDF over Rf interface and includes User-CSG-Information AVP, if PCRF reports CSG-Information-Reporting AVP with CHANGE_CSG_CELL flags.
11. If the policy and charging rule changes cause bearer modification or creation, the P-GW sends a CSG Information Reporting Action IE as part of the Modify Bearer Response, a Change Notification Response, or it can initiate a change through an Update Bearer Request.

Behavior Matrix

Following Message types and the CSG AVP are available in the Gx and Rf interfaces.

Table 11: Message Type behaviour (E-UTRAN/UTRAN)

Message Type	User-CSG-Information AVP (Gx)	User-CSG-Information AVP (Rx)
Create-Session-Request/ Create PDP Context Request	CCR - I	ACR-Start
Modify-Bearer-Request/Update PDP Context Request	CCR-U	ACR-Interim
Change -Notification -Request/MS Info Change Notification Request	CCR-U	ACR-Interim
Delete-Session-Request/ Delete PDP Context Request	-	ACR-Stop
Delete-bearer-Request	-	ACR-Interim/Stop

Note Only 3G and E-UTRAN RAT Type is supported for CSG -information on Gx and Rf Interface.

Handoff Expected Behavior: If there are UE handover from E-UTRAN or 3G to other RAT types (for example. WI-FI) , then the User-CSG-Information AVP will not be sent on Gx and Rf interface.

Monitoring and Troubleshooting

This section provides information regarding show command outputs available for the Closed Subscriber Groups mobility event feature.

Show Commands and Outputs

show subscribers pgw-only full all

The output of **show subscribers pgw-only full all** command has been enhanced to include the following output fields in support of the Closed Subscriber Groups Mobility Event feature on P-GW and GGSN.

Similarly, the output of **show subscribers ggsn-only full all** and **show subscribers saegw-only full** CLI commands has been enhanced to include the following output fields:

Field	Description
UCI	
MCC	Displays a Mobile Country Code (MCC) for User CSG Information.
MNC	Displays a Mobile Network Code (MNC) for the User CSG Information.
CSG-ID	Displays the Closed Subscriber Group identifier.
Access Mode	Displays a matching access mode.
LCSG	Displays Leave Closed Subscribers Group (LCSG) value. The default value is 0.
CMI	Displays CSG Membeship Information (CMI). The CMI displayed is either Member or Non-Member of hybrid cell.

show ims-authorization sessions full all

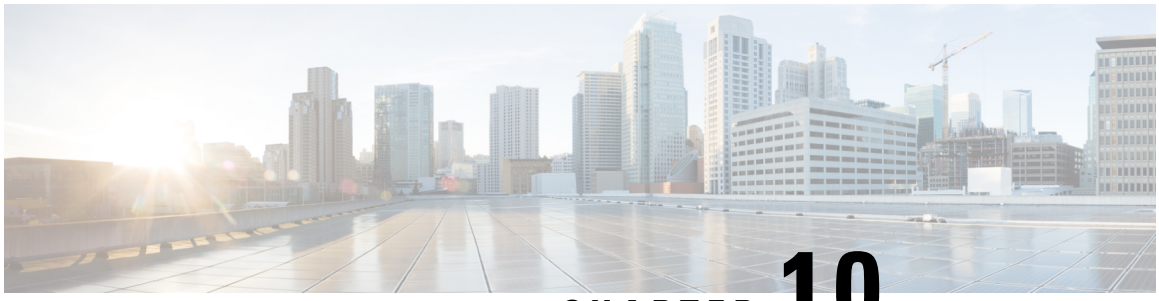
The output of this command has been enhanced to include the following output fields in support of the Closed Subscriber Groups Mobility Event feature on P-GW and GGSN.

Field	Description
Auth Decision:	
Event Triggers:	
User-CSG-Information-Change	Displays total number of User CSG Information change request event triggers.
User- CSG -Hybrid-Subscribed -Information -Change	Displays total number of User CSG Hybrid Subscribed Information.change request event triggers.
User-CSG-Hybrid- Unsubscribed -Information -Change	Displays total number of User CSG Hybrid Unsubscribed Information.change request event triggers..

show ims-authorization service statistics

The output of this command displays the the CSG feature statistics.

Field	Description
Re-Authorization Triggers	
User CSG Info Chg	Displays total number of User CSG Information.change counters.
User CSG Hybrid Sub Info Chg	Displays total number of User CSG Hybrid Subscribed Information change counters.
User CSG Hybrid Unsub Info Chg	Displays total number of User CSG Hybrid Unsubscribed Information change counters.



CHAPTER 10

Crowd Sourcing Optimization

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 - License Required
Related Changes in this Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *Command Line Interface Reference* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First Introduced.	21.23

Feature Description

The Crowd Sourcing Optimization feature uses historical data sessions to provide an increase in recovered capacity from active elephants through seeding profiles and more rapid learning of cell conditions and capabilities.

Crowd Sourcing Optimization feature allows

- Reporting of real-time and historical cell characteristics that capture performances of traffic flows.
- Handling of traffic from the same subscriber by the same session manager.
- Location update enablement.
- Reporting to Cisco Ultra Traffic Optimization library based on the ECGI change instead of ULI change.
- Crowd Sourcing information on each VPP instance.

Note The Crowd Sourcing Optimization feature works only if P-GW learns about user location (for example, from MME). Hence, you should enable the User Location Information update.

Relationship to Other Feature

The Crowd Sourcing Optimization feature is related to Cisco Ultra Traffic Optimization functionality. For details, see the *Cisco Ultra Traffic Optimation* chapter in the *P-GW Administration Guide*.

Licensing

The Crowd Sourcing Optimization feature requires Feature Pack1 license. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

How it Works

The Crowd sourcing optimization procedure describes:

- Handling ECGI Information
- Enhanced elephant detection mechanism
- Trial Mode mechanism

Handling ECGI Information

Following is the workflow for processing ECGI data:

- When P-GW records the ULI information it receives the session creation request.
- P-GW experiences the traffic, recorded ULI information is reported to CUTO during flow creation.
- During the location update, new ULI information is received in bearer modification request during mid flows. All the flows of respective subscribers gets onloaded and new ULI information is reported through CUTO stream modification and streams get offloaded again once rule is matched.

  Under the “CUTO Upgrade Pack 1” license:

  - Reporting of the ULI information is generated based on CUTO algorithm.
  - ULI type and ECGI information gets captured in TODR after the end of flow in multiple phases. It helps for analysis of flows in scale scenario.

Enhanced Elephant Detection Mechanism

Detection of elephant logic, which is based on byte-based, time-based, or bytes-and-time-based thresholds, are added in the configuration CLI as follows.

- Detection mechanism is grouped under the following two modes:
  - **Base Mode**: In Base mode, threshold bytes parameter value is considered.
  - **Enhanced Mode**: In Enhanced mode, combinations of threshold bytes and seed-time values are considered.

  Flows become elephant when either of them crosses first.

Note Seed time is applicable in enhanced mode of detection. Ensure to activate Seed Time and Detection Mode CLI options under the CUTO Upgrade Pack1 license to view all parameters in the CLI.

- Detections of the elephant flows are based on the cuto base policy configuration parameters (seed-time, detection-mode) and CUTO does not consider extended based policy parameters in detection algorithm. CLI throws warning as:

```
Seed-time configured will not take effect for detection. Please configure
under heavy-session” when it’s getting configured.
```

- Detection-cause (time or bytes) and cuto mode (Active/Passive) are recorded in TODR, which helps in the analysis of flows in scale. Detection-cause is recorded under “CUTO Upgrade Pack 1” license and cuto-mode is recorded without any license and applicable for the base CUTO license as well.

Trial Mode

Trail Mode allows the feature to schedule a A/B test campaign from within the P-GW that alternates active and passive modes at regular intervals to demonstrate CUTO’s network efficacy.The Trial Mode operates under the traffic-optimization license or Cisco Ultra Traffic Optimization suppression license, but does not

need the“CUTO feature pack 1” license to turn it on. Service Request (SR) is supported as Trial Mode is applicable only on the Active chassis, however, ICSR is not supported.

Important Make sure to disable Trial Mode before making any changes in the **cuto-profile** because no changes are allowed in the **cuto-profile** during Trial Mode.

Configuring Detection Mode for Elephant Detection Mechanism

Detection of elephant logic that is based on byte-based, time-based or bytes-and-time-based thresholds are added in the configuration CLI as follows.

```
configure
   active-charging service service_name
      [ no ] traffic-optimization-policy policy_name[extended]
         default detection-mode
         detection-mode
        [ no ] heavy-session { standard-flow-timeout  standard_flow-timeout_value
  threshold threshold_value  seed-time seed_time_value }
         end
```

NOTES:

- **default**: Default configuration for detection-mode.
- **detection-mode**: Configures heavy-session detection mode. The default value for detection mode is "enhanced".
- **heavy-session**: Configures heavy-session detection related parameters.
- **seed-time**: Configures time in ms for detection of elephant flow. Use this parameter in the enhanced detection mode.

Configuring Crowd Source Optimization in trial-mode

Use the following CLI commands to enable the Crowd Sourcing Optimization feature in trial-mode.

```
configure
   require active-charging
   active-charging service service_name
      traffic-optimization-profile
         trial-mode  start-time YYYYMMDDHHMM end-time YYYYMMDDHHMM
mode-toggle-interval mode_toggle_interval initial-mode initial_active |
initial_passive
         end
```

NOTES:

- **trial-mode**: Enables the Crowd Sourcing Optimation feature in the Trial Mode.
- **start-time** : Local time begins trial in YYYY:MM:DD:HH:MM.

- **end-time** : Local time ends trial in YYYY:MM:DD:HH:MM.
- **toggle-mode-interval** : Provides interval in minutes to toggle the CUTO mode toggling between Active and Passive at interval. Interval can be at 15, 30, 60 minutes. Starting interval is at 15 minutes.
- **initial-mode** : Set the initial mode with Active or Passive when trial starts.
  - active: Start the trial mode with CUTO mode as active.
  - passive: Start the trial mode with CUTO mode as passive

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the Crowd Sourcing Optimization solution on the P-GW.

Show Commands and Outputs

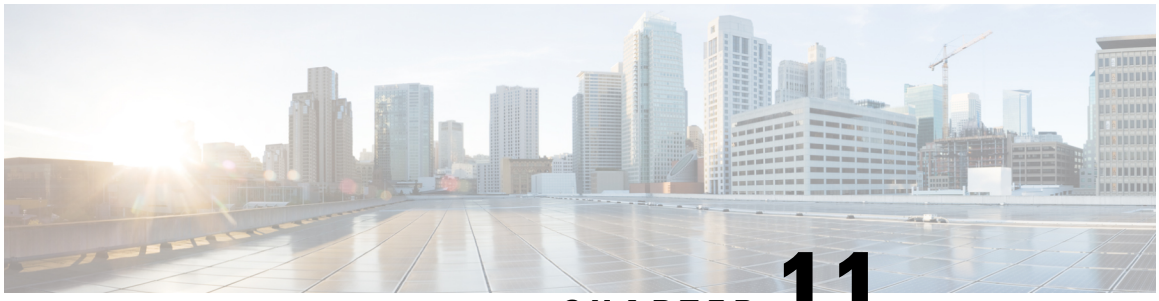
This section provides information about show commands and the fields that are introduced in support Crowd Sourcing Optimization solution.

show active-charging traffic-optimization policy all

Shows configured values of heavy-sessions, extended-heavy-session at active charging service level and traffic optimization policy.

Table 12:

Field	Description
Heavy-Session: Shows heavy-session detection related parameters.	
Seed-Time	Displays time in milliseconds for detection of elephant flow.
Detection-Mode: Shows heavy-session detection mode (Default: enhanced).	
Extended Heavy-Session: Shows heavy-session detection related parameters for extended policy	
Seed-Time	Displays time in milliseconds for detection of elephant flow.



CHAPTER 11

Customizing Last User Location Information

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	• 21.26 • 21.23

Feature Description

Note This is a customer-specific feature. For details, contact your Cisco Account representative.

P-GW CDR does not contain the **lastUserLocationInformation** tag when a dedicated bearer or default bearer session is cleared during the closing session of P-GW CDR for the **custom24** dictionary.

This feature supports the **lastUserLocationInformation** field in the last P-GW CDR when the call is cleared. The **gtpp attribute last-uli** CLI command controls **lastUserLocationInformation** in the P-GW CDR irrespective of whether **gtpp attribute uli** is enabled or not.

Note The **lastUserLocationInformation** field is already supported for **custom52** dictionary but it is not configurable.

Configuring Customized Last ULI

Use the following configuration to customize Last ULI:

```
configure
   context context_name
      gtpp group gtpp_group_name
         [ no | default ] gtpp attribute last-uli
         end
```

NOTES:

- **gtpp group** *gtpp_group_name*: Configures GTPP related parameters for the system to handle a GTPP attribute that does not indicate direction.
- **no | default**: Disables the "Last ULI" field in the CDR.
- **attribute last-uli**: Specifies the optional field "Last ULI" in the CDR.

Monitoring and Troubleshooting

This section provides information to monitor and troubleshoot this feature.

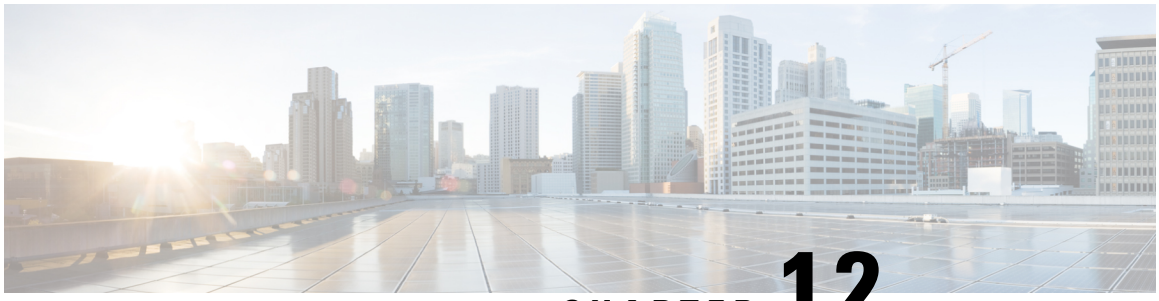
Show Commands and Output

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

show gtpp group name default

The output of this command displays the following field:

Field	Description
Last User Location Information present	Displays "Yes" or "No" to indicate the last user location information.



CHAPTER 12

Customizing TAC Field in CDR

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	• 21.26 • 21.23

Feature Description

Note This is a customer-specific feature. For details, contact your Cisco Account representative.

When a User Location Information (ULI) IE is received, the P-GW stores the information in the P-GW Charging Data Record (CDR). When the ULI IE is updated, the ULI field of the P-GW CDR gets reflected.

However, there are instances where after receiving the initial ULI with TAI + ECGI, the subsequent ULIs receive only ECGI. With this feature, P-GW saves the latest TAC and appends it to the main level ULI field in the P-GW CDR along with ECGI, if TAC is not received.

Examples of ULI customization:

1. Initial ULI received in Create Session Request:TAI + ECGI.
   - TAI > MCC: 214, MNC: 365, TAC: 0x6789
   - ECGI > MCC: 214, MNC: 365, ECI: 0x0001234

   TAC: 0x6789 is saved by P-GW.
2. ULI is modified to ECGI only.
   - ECGI > MCC: 214, MNC: 365, ECI: 0x0003333
   - Whenever ULI is written to P-GW CDR, saved TAC is used
   - ULI in P-GW CDR contains the following:
     a. TAI > MCC: 214, MNC: 365, TAC: 0x6789
     b. ECGI > MCC: 214, MNC: 365, ECI: 0x0003333

Note As LAC is not a separate element in ULI, in case of CGI, RAI or SAI, LAC is expected to be received always.

Configuring Customized TAC

Use the following configuration to customize TAC:

```
configure
  context context_name
    gtpp group gtpp_group_name
      [ no | default ] gttp attribute tac-always-in-uli
      end
```

NOTES:

- **gtpp group** *gtpp_group_name*: Configures GTPP related parameters for the system to handle a GTPP attribute that does not indicate direction.
- **no | default**: Disables the addition of saved TAC to ULI.
- **gttp attribute tac-always-in-uli**: Specifies the "TAI Location Type" option always in the ULI CDR field.

Monitoring and Troubleshooting

This section provides information to monitor and troubleshoot this feature.

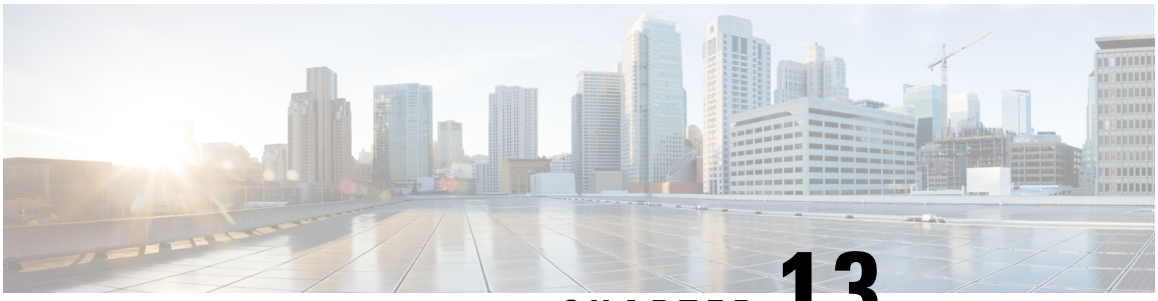
Show Commands and Output

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

show gtpp group name default

The output of this command displays the following field:

Field	Description
TAC Always present	Displays "Yes" or "No" to indicate the presence of TAC in the ULI field of the PGW-CDR.



CHAPTER 13

Diameter Route Table Entries Display Limit and Filtration Enhancement

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW • GGSN
Applicable Platform(s)	All
Feature Default	Not Applicable
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

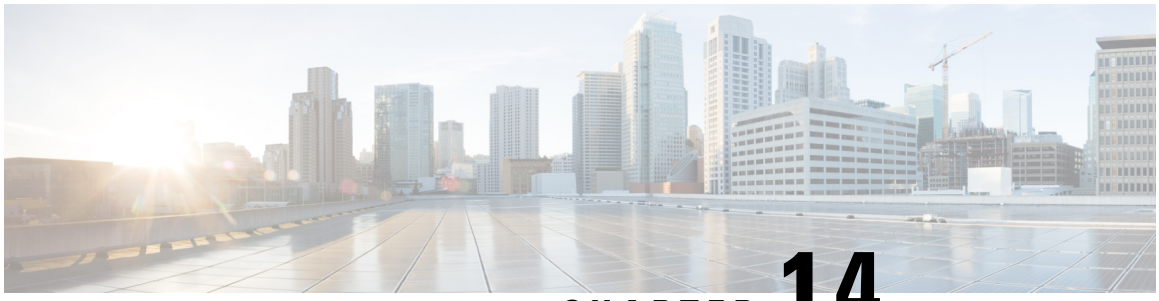
Revision Details	Release
First Introduced.	21.23.12

Feature Changes

Previous Behavior: The CLI output for the diameter route table does not have any limit and filtration on displaying route entries and this resulted to crash and restart of CLI task when there is a huge list of diameter route entries.

New Behavior: A limit is enforced and expired route entries are filtered while displaying the diameter route entries.

Impact on Customer: As the limit and filtration are enforced for the existing CLI **show diameter route table debug-info**, the changes introduced avoids the CLI task crash/reload for the cases where there is a huge list of diameter route entries to be shown/displayed. This limit is applicable for diameter route display during SSD collection and regular CLI **show diameter route table debug-info** execution.



CHAPTER 14

Dynamic Enabling of UBR Buffering in MME Services

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 Documentation	• *MME Administration Guide* • *Statistics and Counters Reference*

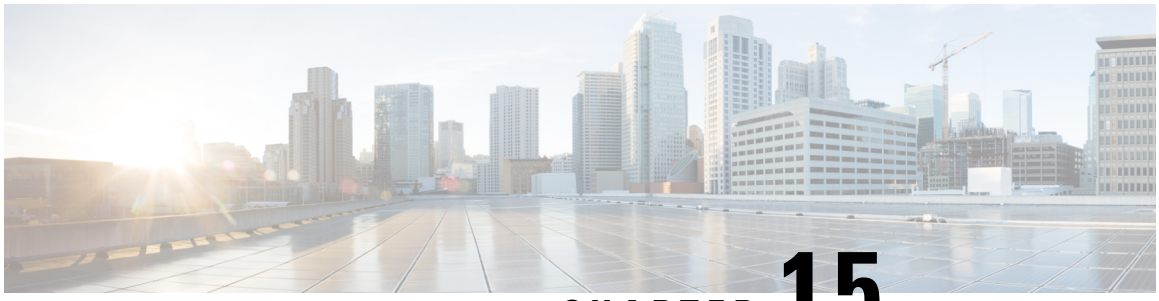
Revision History

Revision Details	Release
First Introduced.	21.23.20

Feature Changes

Previous Behavior: The **buffer-ubreq-from-3g-to-4g** CLI configuration command is not designed for dynamic usage in active mme-service. Enabling the CLI dynamically can restart mme-service and can interrupt active-linked subscribers to the mme-service.

New Behavior: The **buffer-ubreq-from-3g-to-4g** CLI configuration command supports dynamic usage in active mme-service.



CHAPTER 15

Enhanced Event Logging

This chapter describes the MME's Event Logging functionality which occurs at the subscriber level, from the MME to an external server.

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	Enabled- Always-on
Related Changes in This Release	Not applicable
Related Documentation	• *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Customization of Attributes and Events in EDR Profile functionality has been introduced.	21.23.1

Revision Details	Release
First Introduced	21.1

Feature Description

The MME handles numerous subscriber calls from different eNodeBs in the network. In order to troubleshoot any issues for a particular subscriber, the events that caused the issue is recorded. The events could be individual procedures listed below:

- Attach Procedures
- Detach Procedures
- TAU Procedures
- Handover Procedures
- All types of Service Requests
- Paging based on different triggers
- PDN Connectivity Requests
- All types of PDN detach and network initiated PDN detach procedures
- Dedicated Bearer Activation Requests
- Dedicated Bearer Deactivation Requests
- All types of Bearer modification procedures
- CSFB procedures
- SRVCC procedures
- eCSFB procedures
- eSRVCC procedures

The Event Data Record is a proprietary feature of StarOS. In this feature, MME provides a debugging framework to capture procedure level information for each subscriber. On the completion of a procedure successfully or unsuccessfully, the MME generates a procedure summary. This summary provides details of the events and issues, which is nearly comparable to real-time debugging.

Important This feature is license controlled. Please consult your Cisco Account Representative for information about the specific license.

MME supports the following functionality in this feature:

- Event Logging for 4G subscribers.
- The Event Records are stored in CSV file format.
- A framework to collect information and eventually provide log information. The framework is extensible to hold more procedures and information fields.

- The order of fields are not changeable.
- The event logs are generated on completion of the procedure successfully or unsuccessfully. The procedure could be unsuccessful because of local reasons such as – HSS/Peer element triggered reasons, Timeouts for responses, arrival of procedures and so on.
- Each record has a smgr-no and sequence-no field. If there is no guaranteed delivery of events, the sequence number will help in identifying the lost events.
- Event reporting can be enabled or disabled through the CLI command reporting-action mme-event-record under the Call Control Configuration mode. For detailed information on feature configuration see the *Configuring Event Logging* section in this feature chapter.

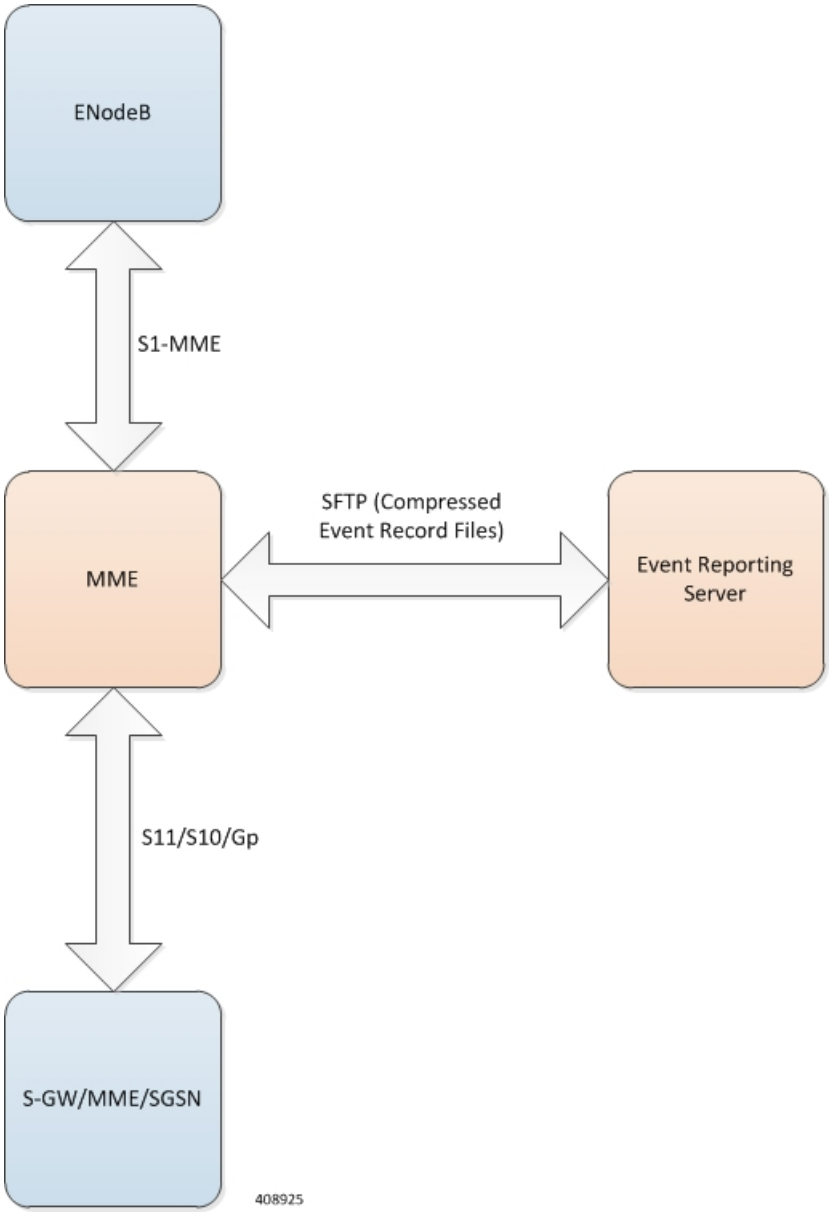
How Event Logging Works

Event Logging in the MME is implemented by providing subscriber event information to an external server. Data analyzers use the event information in the record, which is stored in the external server, to debug and troubleshoot subscriber issues.

Architecture

This section describes the framework designed in the MME to support Event Logging.

Figure 4: Event Logging - Interfaces



The interface between the MME and the external server is based on SFTP. Each record (CSV record) is generated as comma-separated ASCII values. The MME sends one ASCII formatted CSV record per line. The CSV records are stored in a file. If configured, these files can be compressed before sending it to the external server.

The transfer of CSV record files between the MME and the external server is based on either PULL or PUSH model. In case of the PULL model, the external server is responsible for initiating the SFTP with MME, and in the PUSH model, MME is responsible for sending the CSV record file to external server based on the configured PUSH timer interval.

The event report includes the information in CSV format as shown in the table given below.

Table 13: Information Fields in the EDR

Sl.No	Description	Format information	Range
1	smgr_number	Number	1 up to 1023
2	sequence_no	Number	1 up to 4294967295
3	Time	YYYY-MMM-DD+HH:MM:SS	
4	event-idenity	enum: Attach; Detach; TAU; Handover ; Service Request; Paging; PDN Connect/Disconnect; Bearer Activation/Deactivation; CSFB and SRVCC procedures.	
5	Result	enum: 0-Success; 1-failure; 2-Aborted;3-eps_only	
6	mme-address	Dotted-string	
7	Msisdn	String of decimal digits	
8	imsi	String of decimal digits	1 - 15 digits
9	Imei (sv)	String of decimal digits	14 or 16 digits
10	old-guti	mcc: mnc: mmegroup: mmecode: mtmsi	
11	old-guti-type	Enumeration [0 - native, 1 - mapped]	
12	guti	mcc: mnc: mmegroup: mmecode: mtmsi	0 up to 65535
13	Ecgi	mcc: mnc: cellid	
14	current-tac	Tac	
15	enodeB-id	20 bit value	1 - 1048574
16	disc-reason	Number	0 up to 65535
17	ebi	Number	5-15
18	linked-ebi	Number	
19	apn	String	
20	pdn-type	Number	1-4
21	ipv4-address	Dotted String	
22	ipv6-address	Dotted String	
23	pti	Number	1-255
24	qci	Number	1-9,65,66, 69,70,128-254

Sl.No	Description	Format information	Range
25	arp	Number	1-255
26	qos-change	Enum [0-No, 1-Yes]	0/1
27	lai	mcc-mnc-lac	

If a particular information is not relevant for the procedure being logged or if particular information isn't available, the corresponding field of that event record will be left blank. For example, if the IMEI is unavailable after the completion of an Attach procedure, the corresponding field of the EDR record becomes blank.

Important All enumerations will be listed by Cisco for every software release. The external server is designed to be aware of the same listing and to interpret the number accordingly. The event records contain 0-based index value of such enumerations to save space and processing overhead.

The Event IDs that are tracked as part of the EDR logging is shown in the below table:

Events	ENUM Value
Attach Procedures	
MME_EDR_EVENT_ID_EPS_ATTACH	1
MME_EDR_EVENT_ID_EMERGENCY_ATTACH	2
MME_EDR_EVENT_ID_COMBINED_ATTACH	3
MME_EDR_EVENT_ID_EPS_HO_ATTACH	4
MME_EDR_EVENT_ID_ATTACH_TYPE_MAX	
Detach Procedures	
MME_EDR_EVENT_ID_UE_INITIATED_DETACH	51
MME_EDR_EVENT_ID_NW_INITIATED_DETACH	52
MME_EDR_EVENT_ID_HSS_INITIATED_DETACH	53
MME_EDR_EVENT_ID_CSFB_UE_INIT_IMSI_DETACH	54
MME_EDR_EVENT_ID_CSFB_NW_INIT_IMSI_DETACH	55
MME_EDR_EVENT_ID_DETACH_TYPE_MAX	
TAU Procedures	
MME_EDR_EVENT_ID_TAU_SGW_RELOC	101
MME_EDR_EVENT_ID_TAU_NO_SGW_RELOC	102
MME_EDR_EVENT_ID_TAU_COMBINED_SGW_RELOC	103

Events	ENUM Value
MME_EDR_EVENT_ID_TAU_COMBINED_NO_SGW_RELOC	104
MME_EDR_EVENT_ID_TAU_PERIODIC	105
MME_EDR_EVENT_ID_TAU_ATTACH_SGW_RELOC	106
MME_EDR_EVENT_ID_TAU_ATTACH_NO_SGW_RELOC	107
MME_EDR_EVENT_ID_TAU_ATTACH_COMBINED_SGW_RELOC	108
MME_EDR_EVENT_ID_TAU_ATTACH_COMBINED_NO_SGW_RELOC	109
MME_EDR_EVENT_ID_TAU_TYPE_MAX	
Handover Procedures	
MME_EDR_EVENT_ID_S1_HO_SGW_RELOC	151
MME_EDR_EVENT_ID_S1_HO_NO_SGW_RELOC	152
MME_EDR_EVENT_ID_X2_HO_SGW_RELOC	153
MME_EDR_EVENT_ID_X2_HO_NO_SGW_RELOC	154
MME_EDR_EVENT_ID_INBOUND_S10_HO_SGW_RELOC	155
MME_EDR_EVENT_ID_INBOUND_S10_HO_NO_SGW_RELOC	156
MME_EDR_EVENT_ID_INBOUND_S3_HO_SGW_RELOC	157
MME_EDR_EVENT_ID_INBOUND_S3_HO_NO_SGW_RELOC	158
MME_EDR_EVENT_ID_INBOUND_GNGP_HO	159
MME_EDR_EVENT_ID_OUTBOUND_S10_HO	160
MME_EDR_EVENT_ID_OUTBOUND_S3_HO	161
MME_EDR_EVENT_ID_OUTBOUND_GNGP_HO	162
MME_EDR_EVENT_ID_HO_TYPE_MAX	
Service Request Procedures	
MME_EDR_EVENT_ID_SERV_REQ_UE_INITIATED	201
MME_EDR_EVENT_ID_SERV_REQ_NW_INIT_PROC	202
MME_EDR_EVENT_ID_SERV_REQ_EXTENDED	203
MME_EDR_EVENT_ID_SERV_REQ_TYPE_MAX	
Paging Procedures	
MME_EDR_EVENT_ID_PAGING_DDN_TRIGGER	251

Events	ENUM Value
MME_EDR_EVENT_ID_PAGING_DETACH_TRIGGER	252
MME_EDR_EVENT_ID_PAGING_BRR_TRIGGER	253
MME_EDR_EVENT_ID_PAGING_IDR_QUERY_TRIGGER	254
MME_EDR_EVENT_ID_PAGING_PCSCF_RESTORATION	255
MME_EDR_EVENT_ID_PAGING_UE_OFFLOAD_TRIGGER	256
MME_EDR_EVENT_ID_PAGING_SGS_TRIGGER	257
MME_EDR_EVENT_ID_PAGING_GMLC_TRIGGER	258
MME_EDR_EVENT_ID_PAGING_PGW_NODE_RESTORATION	259
MME_EDR_EVENT_ID_PAGING_S102_TRIGGER	260
MME_EDR_EVENT_ID_PAGING_IPNE_QUERY_TRIGGER	261
MME_EDR_EVENT_ID_PAGING_TYPE_MAX	
PDN Connectivity Requests	
MME_EDR_EVENT_ID_PDN_CONN_REQ	301
MME_EDR_EVENT_ID_PDN_EMERGENCY_CONN_REQ	302
MME_EDR_EVENT_ID_PDN_CONN_TYPE_MAX	
UE and Network Initiated PDN Detach	
MME_EDR_EVENT_ID_UE_PDN_DISCONN_REQ	351
MME_EDR_EVENT_ID_MME_PDN_DISCONN_REQ	352
MME_EDR_EVENT_ID_HSS_PDN_DISCONN_REQ	353
MME_EDR_EVENT_ID_NW_PDN_DISCONN_REQ	354
MME_EDR_EVENT_ID_PDN_DISCONN_TYPE_MAX	
Dedicated Bearer Activation Requests	
MME_EDR_EVENT_ID_DED_BEARER_ACT_REQ	401
MME_EDR_EVENT_ID_DED_BEARER_ACT_MAX	
Dedicated Bearer Deactivation Requests	
MME_EDR_EVENT_ID_UE_DED_BEARER_DEACT_REQ	451
MME_EDR_EVENT_ID_MME_DED_BEARER_DEACT_REQ	452
MME_EDR_EVENT_ID_PGW_DED_BEARER_DEACT_REQ	453

Events	ENUM Value
MME_EDR_EVENT_ID_DED_BEARER_DEACT_MAX	
Bearer Modification Requests	
MME_EDR_EVENT_ID_NW_BEARER_MODIF	501
MME_EDR_EVENT_ID_HSS_BEARER_MODIF	502
MME_EDR_EVENT_ID_BEARER_MODIF_TYPE_MAX	
CSFB Prodecures	
MME_EDR_EVENT_ID_CSFB_MO_CALL	551
MME_EDR_EVENT_ID_CSFB_MT_CALL	552
MME_EDR_EVENT_ID_CSFB_MO_PRIORITY_CALL	553
MME_EDR_EVENT_ID_CSFB_MT_PRIORITY_CALL	554
MME_EDR_EVENT_ID_CSFB_MO_EMERGENCY_CALL	555
MME_EDR_EVENT_ID_CSFB_MO_SMS	556
MME_EDR_EVENT_ID_CSFB_MT_SMS	557
MME_EDR_EVENT_ID_ECSFB_MO_CALL	561
MME_EDR_EVENT_ID_ECSFB_MT_CALL	562
MME_EDR_EVENT_ID_ECSFB_EMERGENCY	563
SRVCC Procedures	
MME_EDR_EVENT_ID_SRVCC_SV_CSPS	601
MME_EDR_EVENT_ID_SRVCC_SV_CS	602
MME_EDR_EVENT_ID_SRVCC_SV_NO_DTM	603
MME_EDR_EVENT_ID_SRVCC_1XRTT	604
MME_EDR_EVENT_ID_SRVCC_MAX	

The status of each event is as shown in the table given below:

Table 14: Event Status

Sl No.	Format Information	ENUM Value
1	MME_EDR_EVENT_RESULT_SUCCESS	0
2	MME_EDR_EVENT_RESULT_FAILURE	1
3	MME_EDR_EVENT_RESULT_ABORT	2

SI No.	Format Information	ENUM Value
4	MME_EDR_EVENT_RESULT_EPS_ONLY	3

Support to Add Two Additional Attributes in EDR

In the existing Event Data Record (EDR) fields, there are a total of 27 fields and currently, 2 more fields are added to the event-data-record and they are mme-ue-s1ap-id and procedure-start-time.

The event report includes the information in CSV format as shown in the table given below:

Table 15: Information Fields in the EDR

SI.No	Description	Format Information	Range
28	mme-ue-s1ap-id	Number	0 to 4294967295
29	procedure-start-time	YYYY-MM-DD+HH:MM:SS	

Customization of Attributes and Events in EDR Profile

Feature Description

The Event Data Record (EDR) captures and provides information of each subscriber irrespective of successful or unsuccessful completion of the procedure. The output summary provides the complete details of the events and issues.

There are totally 29 attributes available in the existing EDR fields, and currently there is no option to either customize or choose the number of attributes and EDR events based on the requirement. In this feature, a new EDR-Profile is introduced to enable or disable the events and attributes. Based on the profile configuration, the generated EDR has the events configured and includes the attributes that are enabled and skips the disabled attributes.

This customization of the attributes does not alter the order sequence of the attributes that is already being followed to write into the EDR. In case, if any of the attributes are not configured or not valid/NULL during the particular procedure execution, then it can be included by using just a comma. Maximum of 32 EDR profiles can be configured and only 1 of the EDR profile could be associated per call control profile.

Previously EDR gets generated with event-id as 0 for those procedures for which EDR-Event is not mapped. Currently, EDR does not get generated for those procedures for which EDR-Event is not mapped.

In any condition, if the IMSI is not available since call-control-profile is chosen based on the IMSI, EDR customization is not applicable for such scenarios. If the EDR handle is available, EDR is generated for a list of events/attributes else EDR will not be generated.

Note The top four attributes (*smgr_instance, sequence_no, edr-time, event-Id)* cannot be customized and all the remaining attributes can be enabled and disabled based on the requirement,

Configuring EDR Profile for Set of Attributes and Events

Use the following configuration commands to configure EDR Profile for set of attributes and events:

```
configure
   edr-profile edr_profile_name
       [ no ] attribute attribute-name
       [ no ] event-group event-name
 end
```

Notes:

- **edr-profile**: Configures an EDR profile. *edr_profile_name*: Specifies an EDR Profile name. Enter a string of size 1–63.
- **attribute** : Configures the attribute to be customized.
- **event-group** : Configures the event-group to be customized.
- **no**: Enables or Disables options such as edr-profile, attribute, and event-group.

Associating EDR-Profile with Call-Control-Profile

Use the following configuration commands to associate edr-profile with call-control-profile:

```
configure
   call-control-profile profile_name
       [ remove ][ { reporting-action } { mme-event-record }[edr-profile
edr_profile_name  ) ] ]
     end
```

Show Command and Output

show edr-profile all | full | name

The output of this command displays the configuration of edr profile for all the attributes and event-groups:

1. Attributes-The output displays the following list of attributes enabled or disabled under edr-profile:
2. Event-group-The output displays the following list of events enabled or disabled under edr-profile:

Note By default, all attributes and event-groups are enabled. It can be enabled and disabled based on the requirement.

```
Edr Profile Name : test
Attribute :
result : Enabled
mme-address : Enabled
msisdn : Enabled
imsi : Enabled
imei (sv) : Enabled
old-guti : Enabled
old-guti-type : Enabled
guti : Enabled
ecgi : Enabled
```

```
current-tac : Enabled
enodeb-id : Enabled
disc-reason : Enabled
ebi : Enabled
linked-ebi : Enabled
apn : Enabled
pdn-type : Enabled
ipv4-address : Enabled
ipv6-address : Enabled
pti : Enabled
qci : Enabled
arp : Enabled
qos-change : Enabled
lai : Enabled
proc-start-time : Enabled
mme-ue-s1ap-id : Enabled
all : Enabled

Event-group :
attach : Enabled
detach : Enabled
tau : Enabled
handover : Enabled
service-request : Enabled
paging : Enabled
pdn-connect : Enabled
pdn-disconnect : Enabled
bearer-act-request : Enabled
bearer-deact-request : Enabled
bearer-mod-request : Enabled
csfb : Enabled
srvcc : Enabled
all : Enabled
```

show call-control-profile full name

The output of this command displays the configuration of call-controle-profile for the newly introduced attributes:

Note Ensure that the EDR profile is created before associating it to the call-control-profile. If a non-existent edr-profile is associated to the call-control-profile then edr customization is not applicable.

- Edr Profile: Displays configuration for Edr Profile.
- edr-profile-name/Not Defined: The output of this command displays the associated edr-profile name if configured else it will display as Not Defined.

Limitations

The reliability of event generation is limited by the CDRMOD framework – particularly in the following ways:

- Any reboot of the chassis, will result in loss of records that are not yet flushed to the hard-disk or an external server
- In case of overload of the CDRMOD, the SESSMGR ignores event records if the queue is full.

- EDR sequence numbers are within the scope of the Session Manager. If a different Session Manager is selected, the EDR sequence number may reset or continue from the last sequence number allocated in that Session Manager.
- The statistics are key parameters for logging EDRs, if the statistics have any discrepancies the EDRs are not generated. Listed below are some scenarios where the EDRs are not generated due to discrepancies in statistics:
  - Network or MME initiated dedicated bearer de-activation during SRVCC procedures.
  - HSS initiated modification failures.
  - HSS initiated PDN disconnect failures.
- Currently, MME does not support the event record generation based on the call-control-profile. You can enable the event record generation similarly as enabling at mme-service. You can enable for all subscribers at mme-service or at call control profile. However, the call control profile allows you to enable for all subscribers and not for specific subscribers.

Relationship with Other Products

The SGSN has a similar function, GMM-SM Event Logging. For information about this functionality refer to the *SGSN Administration Guide.*

Configuring Event Logging

The following configurations are discussed in this section for Event Data Records (EDRs):

Enabling Event Logging

The following CLI configuration is executed in the Call Control Profile mode to enable Event Logging on the MME.

```
config
 call-control-profile profile_name
 reporting-action mme-event-record  edr-profile  edr-profile-name
          exit
```

Notes:

- The call-control-profile configuration enables Event Logging for MME, provided this profile is associated to the **mme-service** through operator policy and subscriber map.
- **reporting-action** enables procedure reports.
- **mme-event-record** reports MME procedures in the form of event records using CDRMOD.
- **reporting-action mme-event-record edr-profile edr-profile-name**: Associates an edr-profile in a call-control-profile.

.

Enabling EDR Logs

The CDRMOD proclet writes the individual records into a single file received from several session managers. The CDRMOD proclet is enabled with the configuration below.

```
config
 context context_name
 edr-module active-charging-service reporting
                  cdr { push-interval interval_time | remove-file-transfer
| use-harddisk | transfer-mode { pull | push primary { encrypted-url |
url } url [ secondary { encrypted-secondary | secondary-url } url_ ]  } [
module-only ] }
                end
```

Configuring File Parameters

File parameters can be configured using the configuration given below.

```
config
 context context_name
 session-event-module
                file name file_name current-prefix current_file_prefix rotation
 volume file_rotation_size rotation time file_rotation_time  field-separator
underscore sequence-number padded charging-service-name include compression
 gzip }
              end
```

EDR Profile Association

The Call Control Profile configuration enables event Logging for MME, provided the EDR profile is associated to the MME-Service through Operator Policy and Subscriber Map (LTE-Policy).

```
config
   operator-policy name  policy_name
     associate call-control-profile call_control_profile_name
        exit
lte-policy
    subscriber-map map_name
     precedence precedence_value match-criteria all operator-policy-name
policy_name
          exit
       exit
context context_name
   mme-service service_name
     associate subscriber-map map_name
       end
```

Verifying the Event Logging Configuration

The following commands are used to verify the parameters for Event Logging.

- **show call-control-profile full all**

- **show operator-policy full all**
- **show lte-policy subscriber-map name sub1**
- **show mme-service all**

Monitoring and Troubleshooting Event Logging

This section provides information on how to monitor Event Logging.

Event Logging Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of Event Logging.

The show commands in this section are available in support of the Event Logging.

show call-control-profile full all

```
Call Control Profile Name = TEST
SAMOG Home PLMN                         : Not configured
Accounting Mode (SGW/SaMOG)             : None
Accounting stop-trigger (SGW)           : Not configured
Accounting Policy (SaMOG)               : Not configured
Event Data Records (MME)                : Enabled
```

show edr-profile full all

Following example is the show output of edr-profile.

```
Tuesday April 27 02:06:11 EDT 2021

Edr Profile Name : edr1
***** Attribute *****
result : Enabled
mme-address : Enabled
msisdn : Enabled
imsi : Enabled
imei (sv) : Enabled
old-guti : Enabled
old-guti-type : Enabled
guti : Enabled
ecgi : Enabled
current-tac : Enabled
enodeb-id : Enabled
disc-reason : Enabled
ebi : Enabled
linked-ebi : Enabled
apn : Enabled
pdn-type : Enabled
ipv4-address : Enabled
ipv6-address : Enabled
pti : Enabled
qci : Enabled
arp : Enabled
qos-change : Enabled
lai : Enabled
procedure-start-time : Enabled
mme-ue-s1ap-id : Enabled
all : Enabled
```

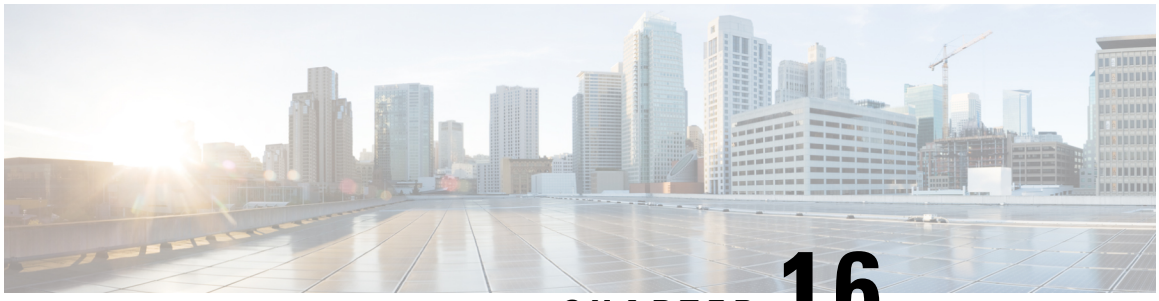
```
***** Event-group *****
attach : Enabled
detach : Enabled
tau : Enabled
handover : Enabled
service-request : Enabled
paging : Enabled
pdn-connect : Enabled
pdn-disconnect : Enabled
bearer-act-request : Enabled
bearer-deact-request : Enabled
bearer-mod-request : Enabled
csfb : Enabled
srvcc : Enabled
all : Enabled
[ingress]asr5500#
```

show cdr statistics

On running the above command , the following statistics are displayed:

```
EDR-UDR file Statistics:
CDRMOD Instance Id: 2
    Overall Statistics:
      Files rotated:
          30
      Files rotated due to volume limit:                                    0
      Files rotated due to time limit:                                        3
      Files rotated due to tariff-time:                                      0
      Files rotated due to records limit:                                 11
      File rotation failures:
   0
      Files deleted:
            7
      Records deleted:
          0
      Records received:
 23754
      Current open files:
       0

Time of last file deletion:                              Sunday November 08 23:32:53 EST
2015
Session-Event Record Specific Statistics:
Session-Event files rotated:                                                  30
Session-Event files rotated due to volume limit:                  0
Session-Event files rotated due to time limit:                      3
Session-Event files rotated due to tariff-time:                    0
Session-Event files rotated due to records limit:              11
    Session-Event file rotation failures:                                  0
    Session-Event files deleted:                                             7
    Session-Event records deleted:                                         0
    Session-Event records received:                                    23754
    Current open Session-Event files:                                      0
Time of last Event file deletion:                Sunday November 08 23:32:53 EST 2015
```



CHAPTER 16

Extraction of IPv4 Addresses Embedded in IPv6 Addresses

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
This feature was introduced in 21.17.16 and now supported in 21.23 and later releases.	21.23

Feature Description

Learning the IPv4 address, which is embedded in IPv6 address through DNS snooping, requires matching of IPv4 format against the address learnt from the DNS response.

In this release, IPv4 extraction is done by enhancing the existing Command Line Interface (CLI) for Well-known prefix and Network-specific prefix. For more information on prefixes, refer RFC6052 document.

After the required changes are done in the CLI, IPv4 address extraction happens and the lookup of IPv4 address is done using the learnt address pool.

Relationships to other Features

This feature is related to DNS Snooping feature. For more information about DNS Snooping feature, refer the *DNS Snooping* chapter in the *ECS Administration Guide.*

License Requirements

The Extraction of IPv4 Addresses Embedded in IPv6 Addresses requires the same DNS Snooping license. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

How it Works

The following procedure describes the steps to be followed for IPv4 address extraction:

1. P-GW monitors all responses sent to the UE.
2. P-GW snoops only the DNS response and identifies all the IP addresses resulting from the DNS response.
3. The first data packet from IPv4 device reaches P-GW.
4. The Session Manager receives data indication and routes the packet to the ACS manager.
5. The ACS manager analyzes the packet and assigns data session for the flow.
6. Prefix matching is done based on the configured prefix.

Based on the matching, IPv4 address is extracted and it is stored in the ACS data session. Then, IPv4 address starts the lookup in the IPv4 address pool and if it matches, then the traffic is matched with the DNS snooping rule. If match does not happen, then it starts to check for other rules.

Restrictions

This section identifies the restrictions to be applied in CLI for IPv4 address extraction.

Prefix-Set Restrictions:

- Allows network-specific prefixes, well-known prefixes but restricts other prefixes.
- Restricts configuring multiple mask values under the same prefix-set.

- Restricts prefix removal from prefix-set, if the same prefix-set is associated with rule base-strip CLI.
- Restricts prefix-set removal, if the same prefix-set is associated with rule base-strip CLI.

Rule base Restrictions:

- Allows network-specific prefixes, well-known prefixes but restrict other prefixes.
- Restricts strip CLI configuration, if rulebase prefix length is not matched to the associated prefix-set mask value.
- Restricts strip CLI configuration, if the rule base associated prefix-set is invalid.
- Restricts strip CLI configuration, if the available prefix-set is empty.

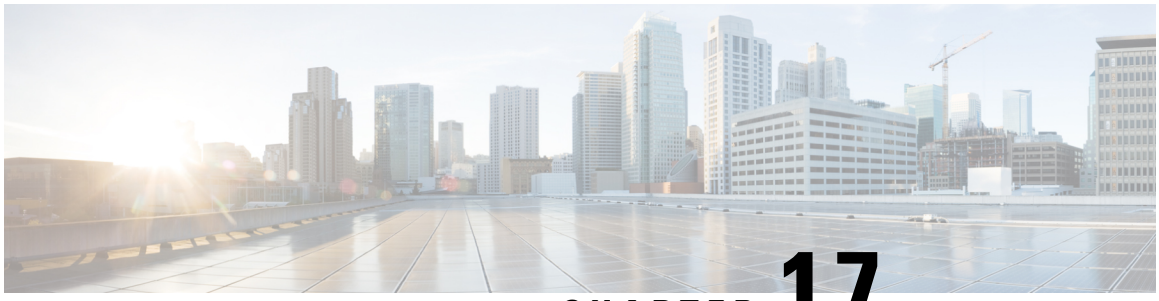
Associating Rulebase to Prefix-Set

Use the following configuration to associate rulebase to the prefix-set.

```
configure
  active-charging service ecs_service_name
    prefix-set prefix_set_name
      exit
    rulebase <rulebase_name>
      strip server-ipv6 prefix_length prefix-set prefix_set_name
      exit
```

NOTES:

- **strip server-ipv6** : Matches the prefix of server IPv6 address with the configured prefixset and prefix length. If match is found then extracts the IPv4 address from the server IPv6 address.
- *prefix_length*: Enter values 32,40,48,56,64 or 96.
- **prefix-set**: Configures the active configuration for Well-known prefix or Netowrk-specific prefix. You can configure a maximum of 10 IPv6 prefixes in a prefix-set.



CHAPTER 17

Failure Counters for CSFB MT Counters

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	Enabled
Related Changes in This Release	Not applicable
Related Documentation	• *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First Introduced	21.23

Feature Description

The Failure Counters for CSFB MT Counters provides a new set of bulkstat counters and modifications to the current Mobile Terminating (MT) Voice-based Circuit Switch Fallback (CSFB) error counters.

The current "csfb-nw-voice-failures" and "csfb-nw-voice-success" counters only capture general failures during the MT CSFB procedures, so it has been requested to extend the MT Voice CSFB counters to capture more specific error scenarios.

This allows the operator to have a more detailed picture of where the errors are occurring in the MT Voice CSFB based procedures.

Monitoring and Troubleshooting

This section provides information on the show commands and Bulk statistics counters.

Show Command and Output

show mme-service statistics csfb-mt-mo-voice-counters

The output of MT Voice CSFB Statistics displays the following new fields:

- MT Voice CSFB Statistics:
  - Attempts/SGSap Paging Requests
  - S1 eNB Paging Timeouts
  - Extended Service Request Rejects
  - SGSap Service Abort Requests
  - S1 UE Init Ctxt Req Setup Fails
  - CS Service Notifications Fails
  - S1 UE Context Modification Fails
  - Miscellaneous Non CSFB UE Ctxt Rel
  - Miscellaneous failures
  - No PS HO Successes

show mme-service statistics mme-service <mme_service_name> csfb-mt-mo-voice-counters

The output of MT Voice CSFB Statistics displays the following new fields:

- MT Voice CSFB Statistics:
  - Attempts/SGSap Paging Requests
  - S1 eNB Paging Timeouts

- Extended Service Request Rejects
- SGSap Service Abort Requests
- S1 UE Init Ctxt Req Setup Fails
- CS Service Notifications Fails
- S1 UE Context Modification Fails
- Miscellaneous Non CSFB UE Ctxt Rel
- Miscellaneous failures
- No PS HO Successes

show mme-service statistics csfb-mt-mo-voice-counters verbose

The output of MT Voice CSFB Statistics displays the following new fields:

- MT Voice CSFB Statistics:
  - Attempts/SGSap Paging Requests
  - S1 eNB Paging Timeouts
  - Extended Service Request Rejects
  - SGSap Service Abort Requests
  - S1 UE Init Ctxt Req Setup Fails
  - CS Service Notifications Fails
  - S1 UE Context Modification Fails
  - Miscellaneous Non CSFB UE Ctxt Rel
  - Miscellaneous failures
  - No PS HO Successes

- CSFB Statistics:
  - UE Initiated Voice Procedures:
    - Attempted
    - Success
    - Failures
  - UE Initiated Priority Voice Procedures:
    - Attempted
    - Success
    - Failures

- NW Initiated Voice Procedures:
  - Attempted
  - Success
  - Failures
- NW Initiated Priority Voice Procedures:
  - Attempted
  - Success
  - Failures
- UE Initiated SMS Procedures:
  - Attempted
  - Success
  - Failures
- NW Initiated SMS Procedures:
  - Attempted
  - Success
  - Failures
- UE Initiated IMSI Detaches:
  - Attempted
  - Success
  - Failures
- NW Initiated IMSI Detaches:
  - Attempted
  - Success
  - Failures

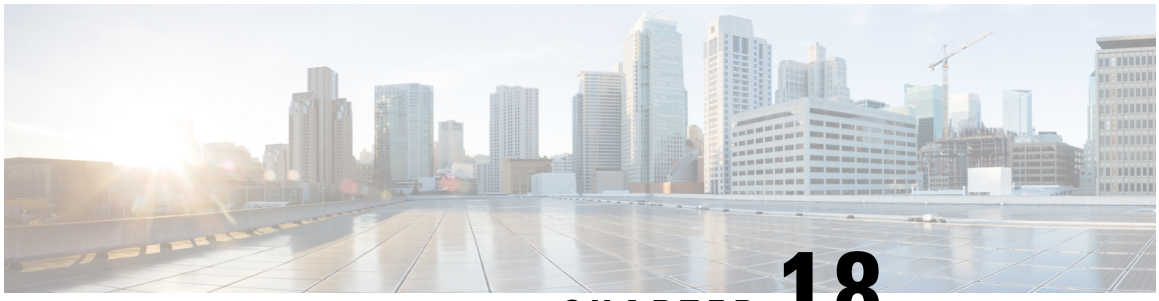
- CS Service Notification

Bulk Statistics

The following set of new MT Voice CSFB bulkstat counters are added in current bulkstat statistic recording mechanism:

Table 16: MT Voice CSFB bulkstat counters

Bulk Statistics Counter	Description
csfb-mt-voice-sgs-paging-request	This counter records all non-retransmitted SGS Paging Requests rx'd from MSC (i.e. The starting point of all the MT CSFB Voice procedures both Idle and Active modes)
csfb-mt-voice-failure-paging-timeout	This counter records max re-transmission timeout failure when eNB/UE do not respond to MME paging request (Idle mode error)
csfb-mt-voice-failure-miscellaneous	This counter records miscellaneous internal errors such as software errors, internal non-delivery errors, internal aborts, message validation errors, collision with start of MO Voice CSFB procedure etc (i.e. Errors not directly linked to the 3GPP spec procedures)
csfb-mt-voice-failure-ext-srv-req-reject	This counter records the failure when the cause code in the Extended Service Request is NOT CSFB Accept (Idle and Active modes)
csfb-mt-voice-failure-init-ctxt-setup	This counter records any Initial Context Setup Response failures encountered during the Idle mode scenario
csfb-mt-voice-failure-cs-notification	This counter records non-delivery/max-retransmission timeout of the CS NOTIFICATION to the UE (Active mode scenario)
csfb-mt-voice-failure-ue-ctxt-mod	This counter records any UE Context Modification failures (either timeout or failure response - Active mode)
csfb-mt-voice-failure-sgs-service-abort-req	This counter records any procedure aborts based on the MT Voice Cancelled flag which is set when rx'ing the SGS service Abort Request from the MSC/VLR
csfb-mt-voice-failure-ue-ctxt-rel-misc	This counter records any other S1 UE Context Release error or cause code that doesn't equal "cs-fallback-triggered = 23" but not the other cause codes stated above (Active mode no HO)
csfb-mt-voice-success-ue-ctxt-rel	This counter records the final success when a S1 UE Context Release response has cause-code "cs-fallback-triggered=23" (Active mode no HO). Successful end-point of the MT CSFB Voice with no HO



CHAPTER 18

Gy Interface Specification for Compliance 2019

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.23

Feature Description

This feature adds support for the Presence Reporting Area (PRA) functionality to comply with the 3GPP standards for Gy interface.

The Presence Reporting Area is an area defined within the 3GPP packet domain for reporting of UE presence within that area. This is required for policy control and in charging scenarios.

Currently, when the PRA information is received, P-GW forwards the Presence Reporting Area Information to the PCRF and this information is not being sent to OCS(Gy).

Following are the specific requirements to support specific Gy interface in P-GW:

1. Presence reporting status : Upon receiving Trigger-Type 73 in CCA-I, P-GW will send Presence-Reporting-Status in CCRU/T towards OCS whenever there is PRA status change reported through S-GW
2. Extended QoS parameters to be sent in CCR messages towards OCS as part of QoS-Information AVP
3. Enhanced-Diagnostics AVP in CCR-T: Report RAN-NAS-Release-Cause Only in CCR-T
4. Support for Multiple Subscription-ID-E.164 ,IMSI and NAI

How It Works

1. The following procedure describes the PRA supporting for Gy interface and its associated behavior:

   During an IP-CAN session, the PCRF determines whether the reports for change of the UE presence in the PRA is required for an IP-CAN session. Then the PCRF determines based on the subscriber's profile configuration and the supported AVP features. The parameter CNO-ULI is set for the same. For the IP-CAN session reporting, the PCRF provides Presence-Reporting-Area-Information AVP, which contains the PRA identifier within the Presence-Reporting-Area-Identifier AVP to the PCEF. For a UE-dedicated PRA, the PCRF provides the list of elements consisting of the PRA within the Presence-Reporting-Area-Elements-List AVP to the PCEF. Presence-Reporting-Area-Elements-List is not currently supported. The PCRF subscribes to the CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48) event trigger at the PCEF at any time during the entire IP-CAN session to activate the reporting changes of the UE presence in the PRA.

   For the same IP-CAN session, the OCS can also determine if the UE presence requires any updates to OCS in Presence-Area-Information AVP. To support this, you must enable the 'trigger pra' config. OCS must send the Trigger-type CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA (73) in Trigger AVP as part of CCA-I towards PGW. The OCS also sends the Presence-Reporting-Area-Identifier in CCA-I (the assumption is that it will same as the PRAID sent from PCRF). PRA reports are then sent towards OCS.

   Upon receiving Trigger-Type 73 in CCA-I, PGW will send Presence-Reporting-Status in CCRU/T towards OCS whenever there is PRA status change reported through S-GW. Presence reporting support is already available for updating Presence Action Start/Stop towards S-GW in CSReq for the Gx interface. For the Gy interface, the same control plane infrastructure is used. A new trigger type is introduced under credit control for the Gy interface so that Trigger Type

-CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA(73) is processed in CCA messages sent from OCS.

When the trigger type CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA (73) is enabled over Gy interface, PRA-IDs are sent to PGW in CCA-I/CCA-U. Whenever there is a PRA status change(MBReq with PRA change), the CCR-U with PRA information AVP is sent to OCS as well.

When the session ends, CCR-T has the PRA information AVP along with the details of the latest PRA-ID and status. At this time the assumption is that Gx and Gy sides would subscribe to the same PRA-ID since it is for the same session. It is also assumed that Gy side subscribe/unsubscribe for a PRA-ID session would not send PRA Start/Stop in CSReq towards SGW since it is already handled from the Gx side. Gy side would only keep a record of PRA-ID for which the presence reporting needs to be sent to the OCS server or not.

2. Extended QoS parameters to be sent in CCR messages towards OCS as part of QoS-Information AVP

   Following extended parameters must be included in the QoS-Information AVP sent to OCS:

   a. Extended-Max-Requested-BW-UL
   b. Extended-Max-Requested-BW-DL
   c. Extended-GBR-UL
   d. Extended-GBR-DL
   e. Extended-APN-AMBR-UL
   f. Extended-APN-AMBR-DL

   When the PCRF has programmed Extended QOS parameters for a particular subscriber, the Extended QOS parameters needs to be sent to OCS in CCR message. The new AVPs sent as part of CCR-Initial/update/Terminate is applicable as per policy updated from PCRF for the specific subscriber.

   ACSMGR has infomation on QoS parameters for the bearer and this is used to send information to DCCA and ultimately OCS server.

3. Enhanced-Diagnostics AVP in CCR-T: Report RAN-NAS-Release-Cause Only in CCR-T

   The Enhanced-Diagnostics AVP (AVP code 3901) is sent in CCR-T message towards OCS and complements the Change-Condition AVP for Offline Charging from PCN Nodes. The RAN-NAS-Release-Cause AVP is under a grouped AVP to allow extensions to other types of release causes in the future.

4. Support for Multiple Subscription-ID - E.164 ,IMSI and NAI

   Multiple subscription ID enables required for various service types under Credit Control Configuration.

   Currently, Multiple subscription ID AVP is encoded in the Gy CCRs based on dictionary and service-type checks. With the subscription ID AVP, customers will have the provision of enabling required Subscription-Id types for various services.

   Each service can have a maximum of three Subscription-Id types (for example: E164, IMSI and NAI) and the advantage of this Multiple subscription ID is that any further dictionary additions in DCCA can be minimized.

Configuring Presence Reporting Area

This section provides information on configuration commands available in support of this feature:

- Configuring PRA (cno-uli) for Gx
- Configuring PRA for Gy

Configuring PRA (cno-uli) for Gx

Use the following configuration commands to enable the PRA:

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        { default | no }diameter encode-supported-features cno-uli
  end
```

Configuring PRA for Gy

Use the following configuration commands to enable trigger-type PRA:

```
configure
  active-charging service service_name
    credit-control group group_name
      trigger-type pra
  end
```

NOTES:

- **pra**: Configures change in ue presence in presence reporting area.

Multiple Subscription ID

Use the following configuration commands to enable the Subscription-Ids for various service types:

```
configure
  active-charging service service_name
    credit-control-group group_name
      subscription-id service-type closedrp ( e164 | imsi | nai }
  end
```

For an instance, if a customer wants E.164, IMSI and NAI value to be encoded in Gy CCR for P-GW service, then the below CLI should be configured in the Credit Control Configuration mode.

```
subscription-id service-type pgw e164 imsi nai
```

NOTES:

- **subscription-id**: Configures Credit Control subscription-ids for service-types.
- **service-type**: Configures Credit Control subscription-ids based on service-types.
- **closedrp**: Configures subscription-id for closedrp service.

Configuring Extended Bandwidth QoS

Use the following configuration commands in Policy Control Configuration to enable the Extended Bandwidth QoS:

```
configure
          context context_name
             ims-auth-service ims_auth_service_name
               policy-control
                  [ no ]diameter encode-supported-features
extended-bw-newradio
     end
```

Show Command and Output

show active-charging sessions full all

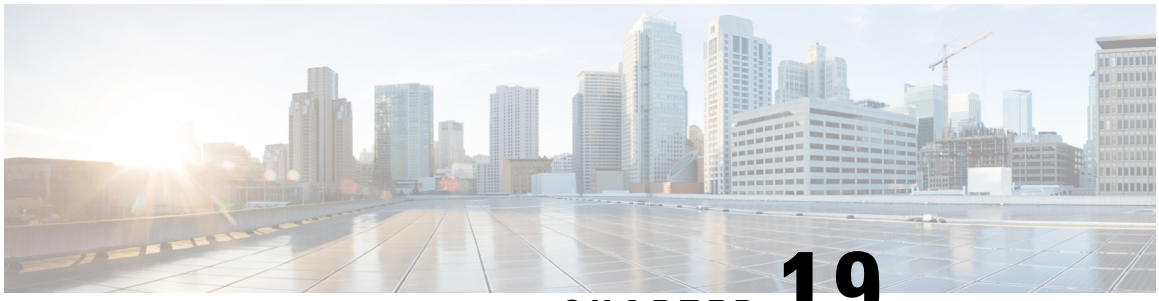
The following new field is displayed to the output of this command:

- Pending Triggers: pra

show active-charging service all | grep pra

The following new fields are displayed to the output of this command:

- Service name
- Credit Control
  - Trigger type:pra



CHAPTER 19

IMS PCO Configurations when Gx is Down

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• S-GW • 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	Not applicable

Revision History

Revision Details	Release
First introduced. **Important** This feature is not validated for all customer deployment scenarios. For more information, contact your Cisco Account representative.	21.23

Feature Description

When Gx is down, the IMS Packet Data Network (PDN) session uses the local policy. However, the existing Proxy-Call Session Control Function (P-CSCF) PCO list configuration under the "ims-auth" profile does not apply to the PDN session within the local policy. The alternative configuration is to configure the P-CSCF IPs under the APN configuration. This APN configuration has a limit of three IP addresses that does not meet the production configuration needs.

The IMS PDN session uses the P-CSCF list configuration under IMSA after falling back to local policy to achieve VoLTE Resiliency. With this feature, the P-CSCF PCO list applies to PDN session in local policy.

How It Works

The UE performs P-CSCF discovery before sending any Session Initiation Protocol (SIP) requests. P-GW provides the UE with the P-CSCF addresses when UE requests the parameters from the network within the Protocol Configuration Options element to include the P-CSCF address. If UE has more than one P-CSCF address, the selection then uses the configuration policy to select the P-CSCF.

Priority of P-CSCF addresses selection in P-GW is as follows:

- Addresses from DNS (S6b provides FQDN or FQDN received from Access Point Name (APN) configuration).
- Addresses from the IMSA-configured table.
- Configuration addresses that are part of APN configuration.

When local policy fallback occurs and Gx is down, P-CSCF list from IMSA profile is used. The following are the scenarios when local policy is used:

- P-CSCF list when Gx is down
- CCR-I Response Failure

Call Flows

The following call flows and procedures explain P-CSCF address selection and Response Failure scenarios.

P-CSCF Address Selection Call Flow

When Create Session Request (CSR) is received with PCO request, the P-GW checks for peers. If all peers are in the down state or no peers are available, then the Gx interface is considered as down. The PDN session fallbacks to the local policy and uses the P-CSCF list from IMSA.

When Virtual APN (VAPN) configuration is available and Gx is down, the P-CSCF uses addresses from IMSA of the selected VAPN. If VAPN configuration is not available, then the P-CSCF address list is received from IMSA of an APN.

Figure 5: P-CSCF Address Selection-Gx Down

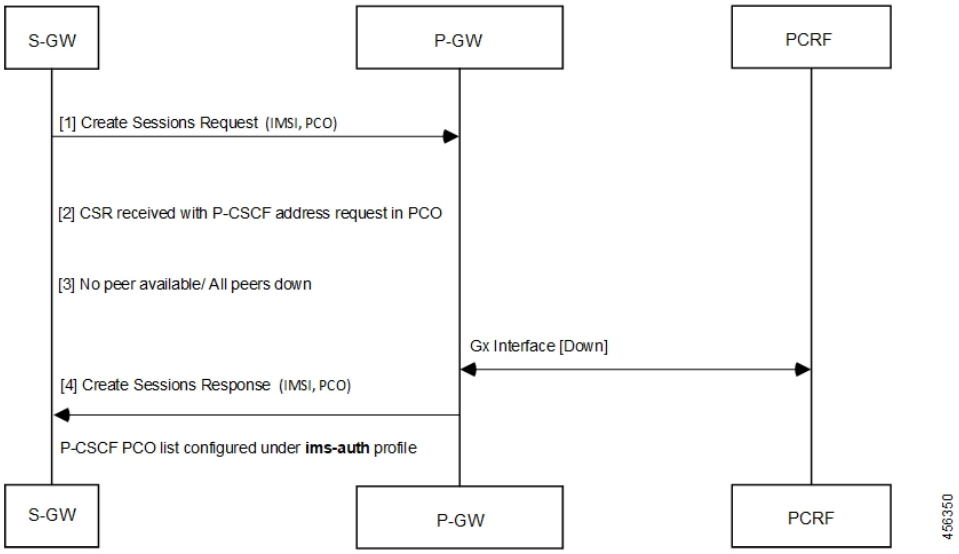


Table 17: Procedure

Step	Description
1	S-GW sends Create Session Request (IMSI, PCO) to P-GW.
2	P-GW receives Create Session Request with the P-CSCF address request in PCO from S-GW and checks for peers available for the Gx interface.
3	If no peers are available or all peers are down, then Gx interface is considered as down between PCRF and P-GW. The PDN session fallbacks to the local policy and uses the P-CSCF list from IMSA.
4	P-GW then sends a Create Session Response with P-CSCF PCO list configurations under the "ims-auth" profile to S-GW.

Response Failures Call Flow

When CSR is received with P-CSCF address request under PCO, the P-GW checks for peers.

If the peer is in the Up state and reachable, Gx is considered in Up state and CCR-I is sent for the primary host. If P-GW receives error response, then the secondary host is used. If the secondary host fails as well, then the PDN session falls back to the local policy and uses the P-CSCF list from IMSA.

Figure 6: Response Failure (CCR–Initial Request)

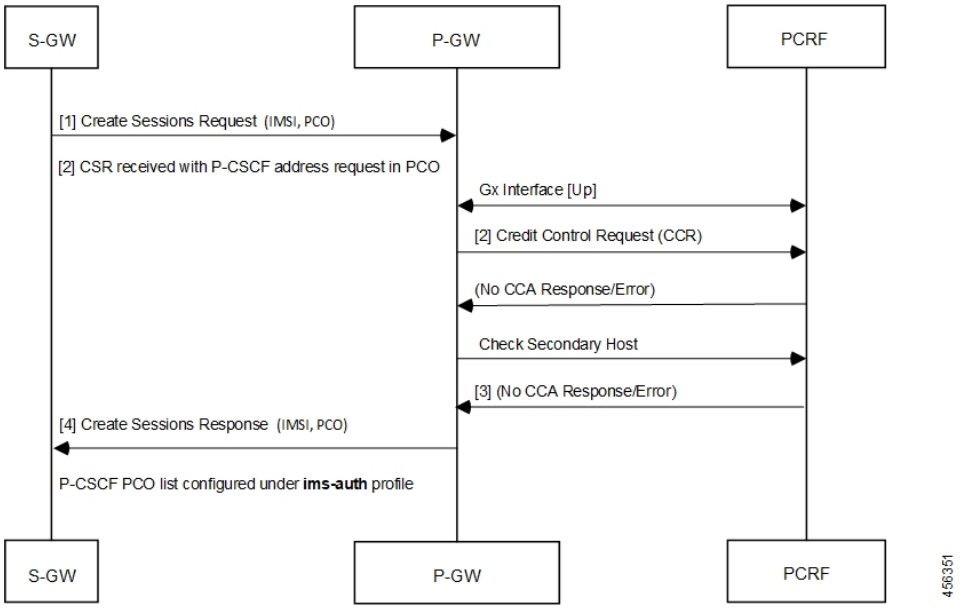


Table 18: CCR-I Response Failure

Step	Description
1	S-GW sends Create Session Request (IMSI, PCO) to P-GW.
2	P-GW receives Create Session Request with the P-CSCF address request in PCO from S-GW and checks for peers available for Gx interface. If the peer is in the Up state and reachable, Gx is in Up state. P-GW sends a Credit Control Request (CCR) to PCRF for the primary host.
3	PCRF does not send credit Control Answer (CCA) Response or sends an error code to P-GW. If case P-GW receives error response, then use the secondary host. If the secondary host fails, then the PDN session falls back to the local policy and uses the P-CSCF list from IMSA.
4	P-GW then sends a Create Session Response with the P-CSCF PCO list configurations under the "ims-auth" profile to S-GW.

Configuring the IMS PCO Configuration when Gx is Down

This section describes how to configure the IMS PCO configuration when Gx is down.

Enabling P-CSCF Address from IMSA in Local Policy Service

Use the following configuration to enable P-CSCF to use the address from IMSA, under Local Policy Service, when Gx is down.

```
configure
  local-policy-service service_name
    [ no ] use-pcscf-config-from-imsa
    end
```

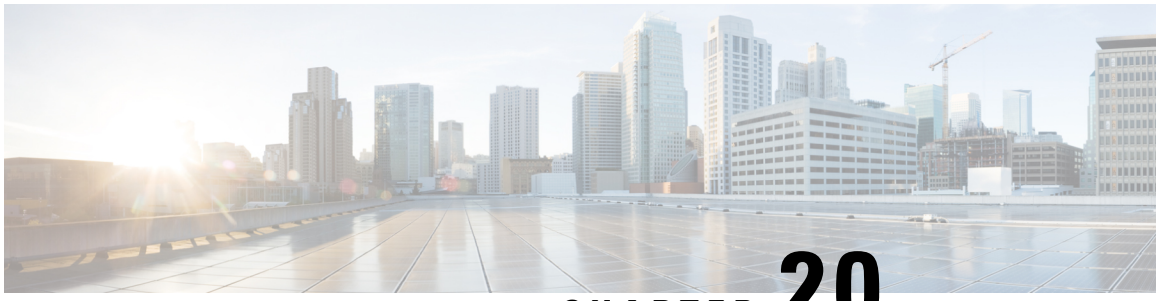
NOTES:

- **no** : Disables the feature.
- **use-pcscf-config-from-imsa**: Specifies to use the P-CSCF configuration from IMSA in Local Policy.
- To define the method of P-CSCF discovery to be used, use the existing **p-cscf discovery** CLI command under IMS Authorization Service Configuration mode.
- To add/append rows with primary and/or secondary IPv4/IPv6 addresses to a P-CSCF discovery table with precedence for P-CSCF discovery, use the existing **p-cscf table** CLI command under IMS Authorization Service Configuration mode.

Verifying P-CSCF Configuration in Local Policy

Use the **show configuration** CLI command to verify if the P-CSCF Configuration in Local Policy is enabled or disabled. The output of this command does not display the mode if the **use-pcscf-config-from-imsa** is disabled.

The **show configuration verbose | grep “use-pcscf” use-pcscf-config-from-imsa** CLI command displays the mode for **use-pcscf-config-from-imsa** when it is enabled.



CHAPTER 20

Increasing Maximum Chunks Per User NAPT for 5G MiFi

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	NAT
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, Modes C - D Reference Guide* • *NAT Administration Guide*

Revision History

Revision Details	Release
In this release, the NAT inline service is enhanced to support utilization of NAT ports and oversubscription configuration.	21.23

Feature Description

The Network Address Translation (NAT) is enhanced to introduce 5G MiFi device to the 5G network. With the enhancement, when more devices are connected to MiFi, the number of flows increases. The new 5G MiFi device allows up to a large number of devices through WiFi that requires the support of a large number of simultaneous IP flows in the P-GW NAT inline service in each single NAT pool. The NAT inline service is enhanced to support oversubscription and to keep a good utilization of NAT ports.

The **min-port-chunk-per-user** parameter added to the NAT ip-pool configuration guarantees new subscriber to have at least 1 (or n) port-chunks allocation. You can configure NAT pool for each subscriber port-chunk number, when it exceeds the calculated port-chunk number based on either (64k port) or **napt-users-per-ip-addres**.

Note

- The **min-port-chunk-per-user** is only applicable to NAPT single-ip.
- **min-port-chunk-per-user** and **port-chunk-threshold** are mutually exclusive.
- Allows over subscription configuration.
- The number of port chunks per IP is reduced when you configure port-chunk size to a higher value. This is because the first 1024 ports are reserved.

For more information about Minimum Port-Chunks Reservation and configurations, refer the *Minimum Port Chunks Reservation* section in the *NAT Configuration* chapter of the *NAT Administration Guide*.

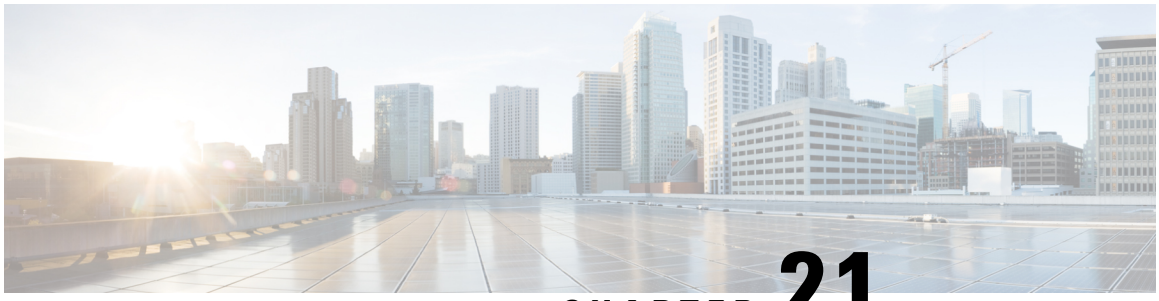
Configuring Many-to-One NAT IP Pools

Use the following configuration commands to configure NAT IP pool.

```
configure
  context context_name
    ip pool min-port-chunk-per-user max_chunks_per_user
    ip pool port-chunk-threshold
    end
```

NOTES:

- **ip pool min-port-chunk-per-user** : Specifies NAT Port minimum number of chunks per user for many-to-one NAT pool. *max_chunks_per_user* must be an integer from 1 through 100.
- **ip pool port-chunk-threshold** and **ip pool min-port-chunk-per-user** are mutually exclusive.



CHAPTER 21

Inter-MME Handover for Modify Bearer Requests without S11-U TEID

Feature Summary an Revision History

Summary Data

Applicable Product(s) or Functional Area	• S-GW • 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	Not applicable

Revision History

Revision Details	Release
First introduced. **Important** This feature is not validated for all customer deployment scenarios. For more information, contact your Cisco Account representative.	21.23

Feature Description

During NB-IoT/Control Plane CIoT EPS Optimization, user data gets transported or SMS messages are passed through MME. This is done by encapsulating them in Non-Access Stratum (NAS), reducing the total number of Control Plane messages when handling a short data transaction. If the Control Plane CIoT EPS Optimization applies, then the MME.

- Indicates S11 interface User Plane (S11-U) tunneling of the NAS user data and sends its own S11-U IP address and MME DL Tunnel End Point Identifier (TEID) for Downlink (DL) data forwarding to the S-GW.
- The S-GW returns a Create Session Response, for Control Plane CIoT EPS optimization, with the S-GW address for S11-U and S-GW TEID. They are used by the MME to forward the Uplink (UL) data toward the S-GW.

In such instances, there might be following constraints:

- S-GW validates Modify Bearer requests (MBR) without S11-U F-TEID.
- If there is no S11-U F-TEID in the MBR, then the S-GW rejects the Inter-MME Handover (HO), since F-TEID is considered mandatory when S11TF flag is set.

To overcome the above constraints and to address the requirements of the IoT devices, the S-GW supports Inter-MME Handover Modify Bearer Requests, without the S11-U TEID functionality, for the NB-IoT subscribers.

How it Works

When the feature is enabled under S-GW Service Configuration mode, the following validation takes place:

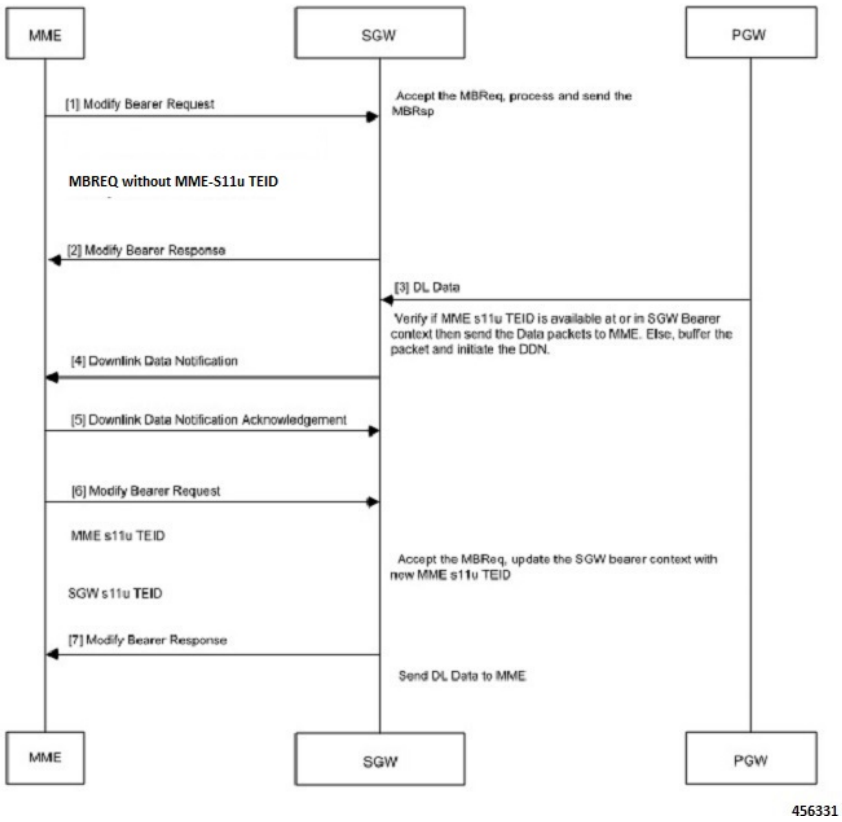
- Handling of IE validation at EGTP Protocol
- Downlink data handling
- Uplink data handling

Call Flow

Handling IE Validation at EGTP Protocol: When Handling IE validation at EGTP Protocol is enabled using the **mme-s11u-without-teid** CLI command under S-GW Service Configuration mode, and the flag is set to be TRUE (default is FALSE):

- The S11-U TEID validation is bypassed.
- The S-GW accepts the Modify Bearer Request and continues the process until handover is successful.

Figure 7: Call Flow for Handling IE Validation at EGTP Protocol



The following table explains the function between MME and S-GW during initial attach procedure.

Table 19: Procedure

Step	Description
1	User Equipment (UE) sends the initial Attach to MME and establishes Control Plane CIoT optimization S11-U EPS bearer with source MME, S-GW, and P-GW.
2	UE moves to the idle state after some time.
3	Source MME releases the S11-U tunnel with S-GW due to no activity.
4	UE moves to Active state in new eNB, and sends Tracking Area Update (TAU) request to the target MME.
5	Target MME uses TAU Request and sends Context Request to source MME.
6	Source MME provides all GTP-C GTP-U F-TEID to the new target MME in Context Response.

Step	Description
7	If the target MME did not send MME GTP-U S11-U TEID, S5/S8 related information inside the Bearer Context of the Modify Bearer Request, Modify Bearer Request from target MME reaches S-GW without any information about MME S11-U TEID and S5/S8.
8	S-GW verifies the Modify Bearer Request it finds S11-U TEID is missing in the request message. As S11-U TEID is considered as mandatory IE, if S11TF flag is set in Modify Bearer Request message. S-GW does not reject modify Bearer Request even if MME S11TF flag is set but MME S11-U-Teid is not present whenever the feature CLI is enabled.

Downlink Data Handling: S-GW receives the Downlink data from P-GW. If MME S11-U TEID is not available in the S-GW bearer context or if the S11-U interface is inactive, the S-GW buffers the DL packets and initiates Downlink Data Notification to MME with the following steps.

Table 20: Procedure

Step	Description
1	Modify Bearer Request Received without MME S11-U TEID.
2	Modifiy Bearer Response sent to MME includes the S-GW S11-U TEID.
3	S-GW receives downlink Data from P-GW on S5/S8 interface.
4	Downlink Data notification is sent to MME.

Uplink Data Handling: S-GW accepts the Uplink data received from the MME and forwards the data to P-GW on S5/S8 interface. For example, the following steps occur at the time of handling Uplink data when Modify Bearer Request is received without the MME S11-U TEID.

Table 21: Procedure

Step	Description
1	Modify Bearer Request is received without MME S11-U TEID.
2	Modify Bearer Response sent to MME includes the S-GW S11-U TEID.
3	Uplink Data is received from MME on S11 interface data tunnel.
4	Uplink Data is forwarded to P-GW on S5/S8 interface data tunnel.

Configuring Inter-MME Handover for Modify Bearer Requests without S11-U TEID

Use the following configuration to enable/disable the Inter-MME Handover for Modify Bearer Requests without S11-U TEID feature.

```
configure
   context context_name
     sgw-service service_name
      [ no | default ] egtp modify-bearer-req accept mme-s11u-without-teid

         end
```

NOTES:

- **default**: Disables the feature. The feature is disabled by default.
- **egtp modify-bearer-req accept mme-s11u-without-teid** : Enables the S-GW to accept MBR without S11u TEID IE present in the Request Message.
- **no**: Disables the feature.

Verifying Inter-MME Handover for Modify Bearer Requests without S11-U TEID Feature Configuration

Use the **show sgw-services name** *sgw_service* or the **show configuration** CLI command to verify if the feature is Enabled or Disabled.

Monitoring and Troubleshooting

This section provides information regarding commands available to monitor and troubleshoot the Inter-MME Handover for Modify Bearer Requests without S11-U TEID on the P-GW/S-GW.

Show Commands and Outputs

The following CLI commands are available in support of the Inter-MME Handover for Modify Bearer Requests without S11-U TEID.

show sgw-service statistics all

The output of this CLI command, and also the **show saegw-service statistics all function sgw** CLI command, has been enhanced to display the following fields.

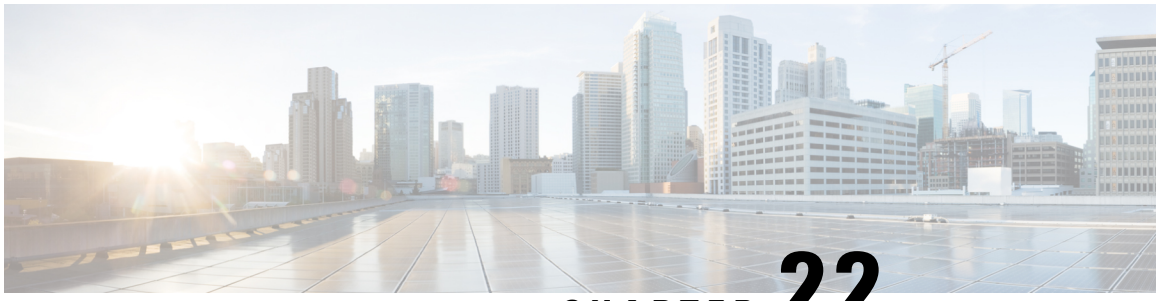
Field	Description
S11-U Buffered Data Statistics Without MME TEID:	
Uplink	Indicates the total number of Uplink data packets that are buffered. **Note** This field is not applicable for the Inter-MME Handover Modify Bearer Requests without S11-U TEID feature.
Total Pkts	Indicates the total number of packets received from MME. **Note** This field is not applicable for the Inter-MME Handover Modify Bearer Requests without S11-U TEID feature.
Downlink	Indicates the total number of Downlink data packets that are buffered at S-GW when there is no MME S11-U TEID.

Field	Description
Total Pkts	Indicates the total number of Downlink packets buffered when there is no MME S11-U TEID.

show egtpc statistics

The output of this CLI command has been enhanced to display the following fields.

Field	Description
Modify Bearer Request Without MME S11u TEID	
Total Rx	Indicates the total number of Modify Bearer Request messages received without MME S11-U TEID Information Element (IE).
Accepted	Indicates the total number of Modify Bearer Request messages accepted without MME S11-U TEID Information Element (IE).



CHAPTER 22

MME Masked IMEISV

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
Related Changes in This Release	Not applicable
Related Documentation	• *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First Introduced	21.23

Feature Description

Some 5G devices do not support 3GPP wireless function as they comply with R15 standard. To make those devices 3GPP compatible, Router Area Network (RAN) requires the model and software information of the specific devices.

MME provides "Masked IMEISV" IE to RAN and makes the unsupported 5G devices compatible for 3GPP wireless functions.

In order to address this device compatibility issue, a new configuration command is introduced in the “mme-service” configuration mode. It enables and disables the sending of the masked International Mobile Station Equipment Identity and Software Version Number (IMEISV) value in the following S1AP messages:

- Initial Context Setup Request
- Handover Request

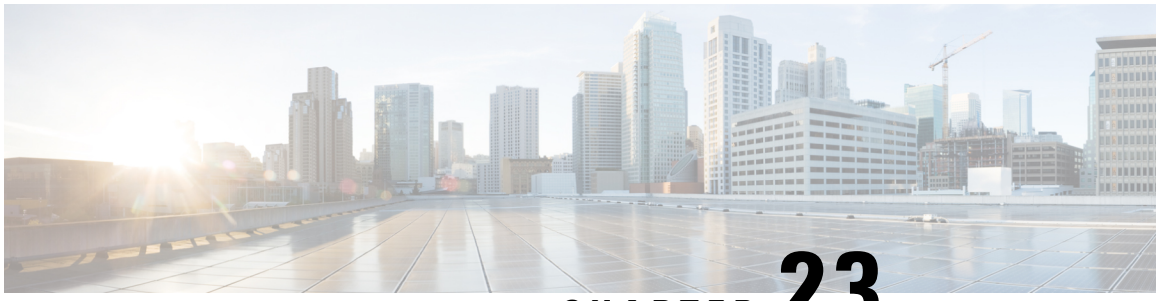
The (IMEISV) is an Optional IE in the S1AP “Initial Context Setup Request” and “Handover Request” messages. The IMEISV is composed of the following elements (each element must be in decimal digits only):

- Type Allocation Code(TAC) and length is 8 digits
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and its length is 6 digits
- Software Version Number (SVN) identifies the software version number of the mobile equipment and its length is 2 digits
- When the masked imeisv flag is enabled, the last 4 digits of the SNR value are converted as ffff before sending . However, the original imeisv value cannot be modified

Enabling and Disabling Masked IMEISV

Use the following configuration commands to enable and disable masked IMEISV in the S1AP messages "Initial Context Setup Request" and " Handover Request":

```
configure
  context context_name
    mme-service service_name
      [ no ] enable-masked-imeisv
     end
```



CHAPTER 23

MME Bearer Request Message Enhancements During Handover Process

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 Documentation	• *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

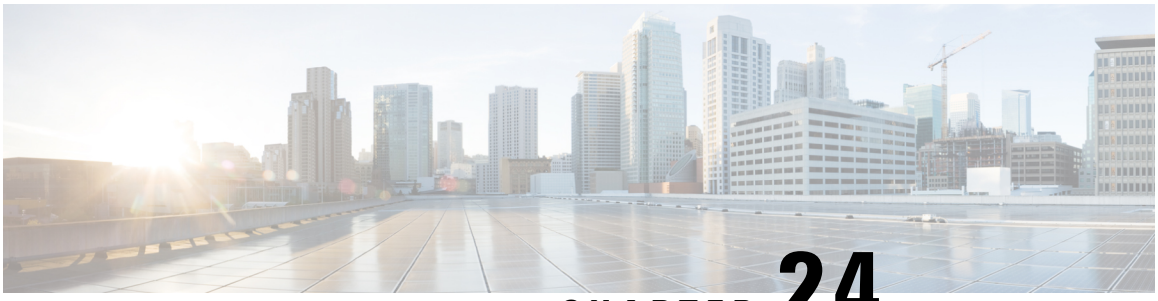
Revision Details	Release
First Introduced.	21.23.20

Feature Changes

Previous Behavior: When the MME receives an update bearer request message during the handover process, it does not buffer update bearer request messages per subscriber at eGTP level.

New Behavior: MME buffers UBRs per subscriber at eGTP level. The **Current Nb of UBRs buffered at mme app** statistics is added under the **show update-bearer-request-stats** to display the current number of UBRs buffered at MME application.

Note After a session manager restart, the session manager is not recovered. It is similar to **Forced_UBResp_CC16_during_HO_3G_4G_TAU_TX** and any other session counters. Hence, this counter is reset after a session manager restart.



CHAPTER 24

Mobile Hotspot Usage on RADIUS Accounting

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
In this release, P-GW supports Mobility Hotspot (MHS) usage on RADIUS accounting.	21.23

Feature Description

In RADIUS Accounting, the subscriber data usage is monitored using the Type Length Values (TLV) namely Acct-Input-Octets and Acct-Output-Octets to receive a cumulative data usage report. In this StarOS 21.23 release, to identify Data usage differentiation effectively in RADIUS accounting for 4G Mobile Hotspot (MHS) data usage, 5G MHS data usage, and 5G composite data usage the following new TLVs are introduced:

- 4G_MHS_Acct_Input_Octets
- 4G_MHS_Acct_Output_Octets
- 5G_MHS_Acct_Input_Octets
- 5G_MHS_Acct_Output_Octets
- 5G_Comp_Acct_Input_Octets
- 5G_Comp_Acct_Output_Octets

RADIUS interim and stop messages report MHS data usage . MHS data usage reporting is allowed per bearer. These TLVs comprises of the cumulative values from the previous interim messages and raw bytes.

When MHS data usage reporting is dynamically enabled or disabled, the change takes effect only for the new calls.

Note Only EUTRAN and NB_IOT Radio Access Technology (RAT) types are supported for MHS data usage reporting.

The PRA IDs that are configured in a PRA profile which are associated with APN level are used to identify 5G data usage.

Relationship with Other Features

This feature is related to Smartphone Tethering Detection Support feature. For more information about Smartphone Tethering Detection support, refer the *PDN Gateway Overview* chapter in the *P-GW Administration Guide*.

License Requirements

The Mobile Hotspot usage on RADIUS Accounting feature requires enabling of Tethering Detection License. Contact your account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the Software *Management Operations* chapter in the *System Administration Guide*.

Limitations

The following is the known limitations of the feature:

- The MHS supports only dictionary custom76.

Configuring MHS Usage on RADIUS Accounting

This section provides information on configuring MHS Usage on RADIUS accounting.

Configuring PRA Profiles

Use the following command to configure PRA profiles to differentiate traffic.

```
configure
          context context_name
            pra-profile pra_profile_name
             [ no ] pra-id pra_id_value traffic-map-type type_value
          end
```

NOTES:

- **pra-profile**: Configures PRA profiles to differentiate traffic.
- **pra-id**: Configures the PRA ID.
- **no**: Removes the PRA ID.
- **traffic-map-type** : Configures the traffic map type.
- **type_value**: Enter enum values - 5G.

NOTES:

A maximum of three PRA IDs per PRA list and associate PRA list in APN level are allowed to differentiate 5G traffic.

Associating PRA Profiles at APN Level

Use the following CLI commands to associate PRA profiles at APN level:

```
configure
  context context_name
    apn apn_name
      [ no ] pra-profile profile_value
 exit
```

NOTES:

- **apn**: Configures the APN.
- **pra-profile**: Associates PRA profiles at APN level.
- **no**: Removes PRA profiles at APN level.

Configuring AAA Group

Use the following commands to configure AAA Group for the newly-added TLVs to send RADIUS Accounting messages.

```
configure
          context context_name
            aaa group group_name
              [ no ] radius accounting mhs-traffic enable
```

```
    radius dictionary custom76
end
```

NOTES:

- **mhs-traffic**: Specifies MHS data usage reporting.
- **enable**: Enables MHS data usage reporting.
- **no**: Disables MHS data usage reporting.

Monitoring and Troubleshooting

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

Show Commands and Output

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

show subscribers pgw-only full all

The output of the **show subscribers pgw-only full all** command displays the following details:

Field	Description
4G MHS Input Bytes	The total number of input bytes used with 4G Tethering.
4G MHS Output Bytes	The total number of output bytes used with 4G Tethering.
5G MHS Input Bytes	The total number of input bytes used with 5G Tethering.
5G MHS Output Bytes	The total number of output bytes used with 5G Tethering.
5G Composite Input Bytes	The total number of input bytes used with 5G Composite (Tethering and non-Tethering).
5G Composite Output Bytes	The total number of output bytes used with 5G Composite (Tethering and non-Tethering).

show subscribers saegw-only full all

The output of the **show subscribers saegw-only full all** command displays the following details:

Field	Description
4G MHS Input Bytes	The total number of input bytes used with 4G Tethering.
4G MHS Output Bytes	The total number of output bytes used with 4G Tethering.
5G MHS Input Bytes	The total number of input bytes used with 5G Tethering.

Field	Description
5G MHS Output Bytes	The total number of output bytes used with 5G Tethering.
5G Composite Input Bytes	The total number of input bytes used with 5G Composite (Tethering and non-Tethering).
5G Composite Output Bytes	The total number of output bytes used with 5G Composite (Tethering and non-Tethering).

show apn name

The output of the **show apn name** command displays the following details:

Field	Description
pra-profile Name	Specifies the PRA name to be associated in APN for differentiating 5G traffic..

show aaa group name

The output of the **show aaa group name** command displays the following details:

Field	Description
Allow accounting MHS Traffic	Enables reporting MHS Data usage in RADIUS accounting messages.

show pra-profile name

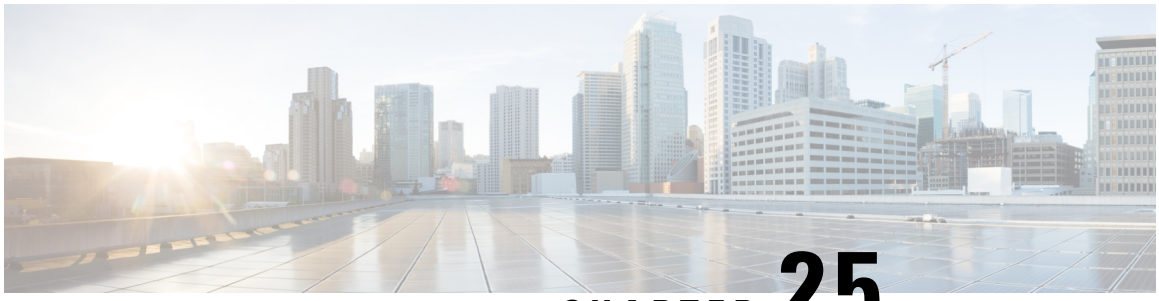
The output of the **show pra-profile name** command displays the following details:

Field	Description
pra profile name	The PRA profile name to be associated in APN for differentiating 5G traffic.
Context	The context name.
PRA Id	The PRA ID to be associated in APN.
Traffic mapping type	The 5G traffic map type.

show pra-profile all

The output of the **show pra-profile all** command displays the following details:

Field	Description
pra profile name	The PRA profile name to be associated in APN for differentiating 5G traffic.
Context	The context name.
PRA Id	The PRA ID to be associated in APN.
Traffic mapping type	The 5G traffic map type.



CHAPTER 25

Password Expiration Notification

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
P-GW supports no-lockout password feature after the expiry of user account passwords.	21.26
This feature is enhanced with a new option to the **save config** command. The enhancement supports downgrade and ensures that the user profiles do not get lost after downgrade.	

Revision Details	Release
In this release, P-GW supports password expiration notification to Context, AAA, and RADIUS users.	21.23

Feature Description

In StarOS, if the password is not reset before the expiration date, you get locked from the P-GW. You are allowed to log on back only when the password is reset by the administrators manually.

StarOS is enhanced to provide password expiration notification to Context, AAA, and RADIUS users. P-GW supports configuration and expiration of passwords for Administrators, Config Administrators, Inspectors, and Operators. The following provisions are supported:

- Specify the password warning interval - It gives a warning to the user about password expiry.
- Specify the password grace interval - During this grace interval the user can change the password by themself rather than approaching the Administrator every time.
- Warning interval and Grace interval have a global configuration under a context. If the user level configuration does not specify either of these values, the global values under the context take effect.

The default values of the parameters are according to Security Guidelines.

- Expiry Interval – Maximum age of the password (90 days default).
- Warn Interval – Warning period before password expiry (30 days default). You get a warning about approaching password expiry. You can continue without changing the password.
- Grace Interval – Days after password expiry, you can use the old password. Beyond the grace period, you are not able to log in with the old password. Admin has to reset the password for you.

For example:

```
login: xxx
password: xxx

Case 1: [Normal]
# {you are logged in}

Case 2: [When in warning period]
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

Case 3: [when in grace period]
Your password has expired
Current password:
New password:
Repeat new password:

Case 4: [after the grace period]
Password Expired (even beyond grace period, if configured). Contact Security Administrator
to reset password
```

Upgrade and Downgrade Process for Password Expiration Notification

The Password Expiry Notification feature keywords in Subscriber configuration supports the **max-age**, **exp-grace-interval**, and **exp-warn-interval**. These new parameters are configured at the Context Global level. Context Global level parameters are used when the per user level configuration is not configured with a default value. For example, for the **max-age** of the password, the default value is 90 days.

For the user profiles with no expiry-date at per user level, startup config takes an expiry date of 90 days for that user. This problem can be solved by manually editing the startup configuration file, but this solution leads to issues when users are distributed across locations.

If downgrade is needed, user profiles are lost as new keywords are not valid for older releases.

Password Lockout Enhancements

The upgrade procedure is updated, and the downgrade process is changed with the help of new **save config** CLI option, **legacy-password-expiry**.

Use the CLI configuration command **lockout-password-aging** to identify whether local users are locked out due to the expiry of their password or not. This password enhancement feature allows local users to login to P-GW without administrators help to manually reset their passwords.

Upgrading and Downgrading Procedures Using Save Configuration Command

Use the following upgrade process:

- Before upgrade, add the **[no] password max-age** command at context level, in all contexts where users are configured in the startup configuration.
- When reloading with image using the updated startup config, all users that are configured without an expiry date will pickup the context level configuration by default and set the user level **no-max-age** keyword automatically.

Use the following downgrade process:

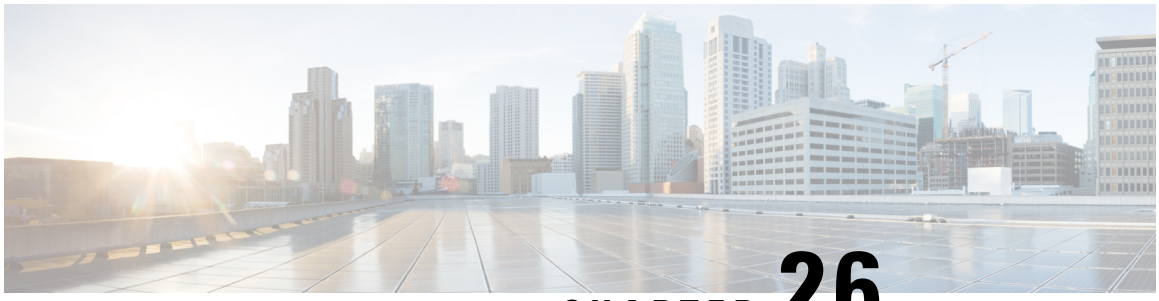
Use the **legacy-password-expiry** CLI command in the **save config** command, based on which new keywords are not saved. Configuration is stored in a format which previous release recognizes.

Use the following configuration under context configuration:

```
configure
  context host_name
    save configuration url [ obsolete-encryption | showsecrets | verbose
 ] [ -redundant ] [ -noconfirm ] [ legacy-password-expiry ]
```

NOTES:

- **save configuration** *url* **legacy-password-expiry**: Generates a backward compatible file by removing the expiry notification keywords. The **save config** command makes the configuration compatible with older versions.



CHAPTER 26

P-GW Buffering Mechanism

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	Enabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, P-GW supports Buffering Mechanism feature.	21.23
First introduced.	21.14

Feature Description

The P-GW can buffer a maximum of two policy (PCRF) messages when the Default-Bearer-QoS change is in pending state. With Presence Reporting Area (PRA) related call flows, two or more messages can be received when the Update Bearer Response (UBResp) is in pending state.

The P-GW Buffering Mechanism feature enables the P-GW to gracefully handle the RAR or CCA-U received from the PCRF when P-GW waits for the UBResp. Once the UBResp is received, the pending messages are fetched from the P-GW Buffer Queue for further processing.

How It Works

Under Active Charging Service (ACS) mode, a CLI command - **pending-buffer-size**, is added to increase the buffer size. The PCRF messages are buffered until the P-GW receives a UBResp message while the Default-Bearer-QoS change is in pending state.

Configuring the P-GW Buffering Mechanism Feature

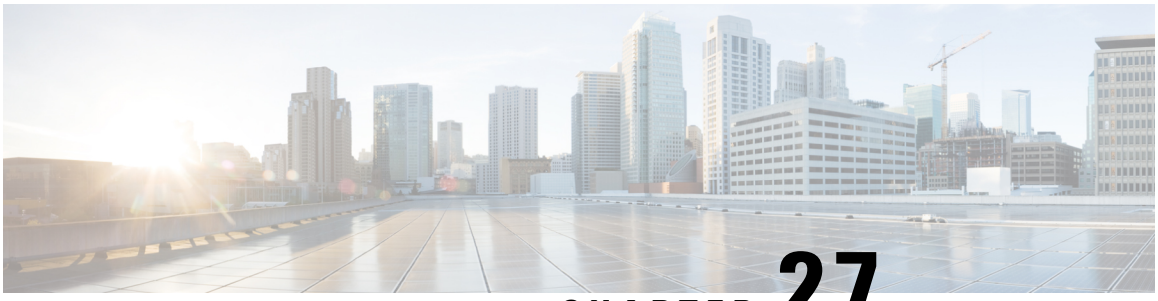
Use the following configuration to increase the buffer size for storing PCRF messages when the Default-Bearer-QoS change status is in pending.

```
configure
  active-charging service service_name
    policy control def-bearer-qos-change pending-buffer-size buffer_size
    end
```

NOTES:

- **def-bearer-qos-change**: Sets the Default-Bearer-QoS change parameters.
- **pending-buffer-size** *buffer_size*: Specifies the buffer size for storing the PCRF messages when Default-Bearer-QoS change is pending. The buffer_size is an integer ranging from 2 through 4.

  The minimum configured value is 2 and maximum is 4.
- The **no policy control def-bearer-qos-change** configures the command with its default setting. Default = 2.
- The default value suffices for most use-cases. However, higher values must be configured based on the use-case basis and by considering the memory usage.
- The CLI command takes effect for new calls.



CHAPTER 27

P-GW Buffering Optimization

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	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *P-GW Administration Guide*

Revision History

Revision Details	Release
In this release, P-GW supports Buffering Optimization to handle PRA messages efficiently.	21.23

Feature Description

The P-GW Buffering Optimization enables the P-GW to handle the Presence Reporting Area (PRA) messages efficiently. When two or more PRAs are received, while UBResp is still pending, there are chances that P-GW buffer queue can become full or even a message drop can happen. This enhancement enables the PRA response from Policy and Charging Rules Function (PCRF) to be handled efficiently as the chances of message drop is less.

When a new message arrives, the P-GW merges the message with the existing similar type of message in the queue. This allows the P-GW to process similar type of messages at the same time without increasing the queue size and reducing the message drop ratio. When messages are read from the queue, the Gx Rule Level Attribute -value pairs (AVPs) defined actions are triggered. The Rule Level AVPs validity is not checked when messages are buffered.

Relationship to Other Feature

The P-GW Buffering Optimization feature is related to P-GW Buffering Mechanism functionality. For details, see the *P-GW Buffering Mechanism* chapter in the *P-GW Administration Guide*.

How it Works

Under Active Charging Service (ACS) mode, a CLI command - **optimze-update** is enabled or disbaled to enable or disable the buffering mechanism.

Configuring the P-GW Buffering Optimization

Use the following configuration to enable or disable the P-GW buffering optimization to process the similar type of messages in the queue.

```
configure
          active-charging service service_name
            [ no ] policy control optimze-update pra-change
        end
```

NOTES:

- **optimize-update**: Enables the optimization for multiple policies received from PCRF, when the earlier response is pending. Default is Disabled.
- **no**: Disables the optimization for multiple policies.
- **pra-change**: Enables policy optimization only during the Presence Reporting Area (PRA) change.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show Active-Charging Sessions Full All

The output of the Show Active-Charging Sessions Full All.

Table 22: show active-charging sessions full all Command Output Descriptions

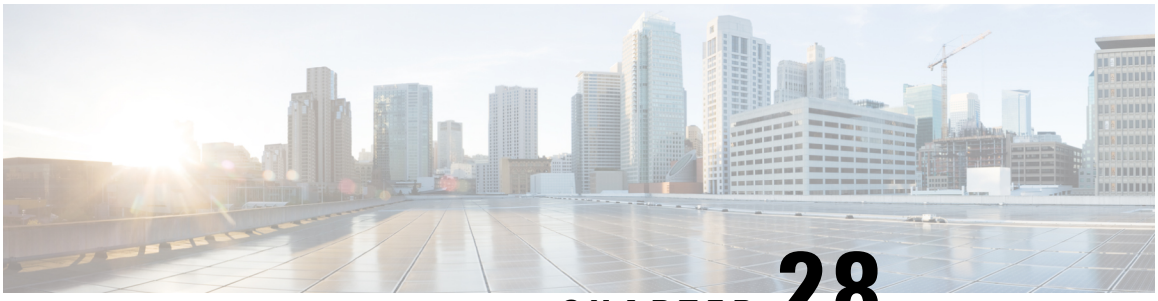
Field	Description
Current P-GW-Buffer Queue Length	Displays the currently utilized queue length.
Total P-GW Buffer Merge Count	Displays the merged count of PRA messages.

show Active-Charging Service All

The output of the Show Active-Charging Service All.

Table 23: show active-charging service all Command Output Descriptions

Field	Description
optimize-update	Enables multiple policy optimization.
pra-change	Enables optimization policies for PRA changes.



CHAPTER 28

PLMN Level Statistics for ePDG Services

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• ASR 5500 • ASR 5700 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *ePDG Administartion Guide* • *Command Line Interface Reference* • *Statistics and Counters Reference,Guide*

Revision History

Revision Details	Release
ePDG supports PLMN level statistics for ePDG services.	21.23

Feature Description

The ePDG level statistics that are available at the ePDG system level do not allow operators to pinpoint issues to certain users of the network. PLMN-based statistics are captured in the CLI and bulk statistics to help operators to localize failures to a particular circle. The PLMN-based statistics allows operators to decide on the load that is generated on the ePDG from different circles and helps in network planning.

- ePDG extracts the PLMN information, such as MCC and MNC from IMSI received in the IKE AUTH Request message.
- ePDG associates a PLMN list with epdg services to enable the collection of PLMN level statistics for all the PLMNs present in the list.
- Displays PLMN statistics in CLI through mandatory options of MCC and MNC.
- Facility to clear the PLMN-based statistics for all PLMNs and for a given PLMN.
- The PLMN statistics is applicable only for the combination of Diameter-based authentication with AAA on SWm interface and GTPv2 based S2b interface.

Configuring PLMN-list

Use the following PLMN list command to capture the statistics at PLMN level. PLMN level statistics will be captured, only if the IMSI received during initial attach / Handoff belongs to one of the PLMNs in the associated PLMN list. By default no PLMN list is configured.

```
configure
   context context_name
      plmn-list plmn_list_name
         mcc mcc_value  mnc mnc_value
         end
```

- **plmn-list**: Configures a list of PLMNs (MCC and MNC) and association to samog-service is required for capturing PLMN level statistics. A maximum of 25 PLMNs are allowed in a list. You can create a maximum of 10 PLMN lists for each context.
- **plmn_list_name**: Enter a name of size 1 to 63
- **mcc** *mcc_value*: Configures the PLMN MCC in the PLMN list. Enter a number, ranging from 100 to 999.
- **mnc** *mnc_value*: Configures the PLMN MNC in the PLMN list. Enter a number, ranging from 00 to 999.

Note List of MCCs with 3 digit MNCs are:

300 302 310 311 312 313 316 334 338 342 344 346 348 354 356 358 360 365 376 405 708 722 732

If you enter MCC, which is present in the above list, then MNC shall be of 3 digits. If you enter a 2-digit MNC for this case, then '0' shall be prefixed to it and stored in the memory. When "show plmn-list name plmn-name" command is executed, then MNC with prefixed '0' is displayed in the output.

Similarly, if user enters MCC which is NOT present in the above list, then MNC shall be of 2 digits. If user enters a 3-digit MNC for this case (with '0' prefixed), then the prefixed '0' shall be removed and stored in the memory. When "show plmn-list name plmn-name" command is executed, then MNC without prefixed '0' is displayed in the output. If the entered MNC is more than 99, then error message is displayed.

For all other combinations, it shall be stored and displayed as it is.

Associate PLMN List to ePDG Services

Use the following command to associate the PLMN List with the ePDG service. ePDG captures the statistics at PLMN level if the IMSI received during initial attach / Handoff belongs to one of the PLMNs in the associated PLMN list. Each ePDG service can have only one PLMN list associated at any given point of time. If there is a PLMN list already associated, a new PLMN list can be associated to a service only after disassociating the existing associated PLMN list.

```
configure
  context context_name
    epdg-service service_name
      [ no ] associate plmn-list  plmn_name
      end
```

Notes:

- **associate plmn-list** *plmn_name* : Associates PLMN lists with ePDG services.
- **[no] associate plmn-list** : Dis-associates the PLMN List with ePDG services and clears the existing PLMN statistics, if present for the PLMNs in the list.

Removing PLMN List Configuration

Use the following command to remove the PLMN list. This command stops SaMOG or ePDG from capturing the statistics at PLMN level and clears the existing PLMN statistics if present for that PLMN.

```
configure
  context  context_name
    no plmn-list   plmn_name
    end
```

NOTES:

- **no plmn-list** *plmn_name* : Removes the PLMN list and stops the PLMN level statistics collection for that PLMN.

Add or Remove PLMN to or from PLMN list

Use the following command to add or remove PLMN to/from PLMN list.

```
configure
   context  context_name
     plmn-list   plmn_name
          no  mcc   mcc_value mnc mnc_value
          end
```

NOTES:

- **no mcc mnc**: Removes PLMN entry with MCC and MNC combination from PLMN list. This commnad clears existing statistics if present for that PLMN.
- **mcc** *mcc_value* **mnc** *mnc_value*: Adds or removes the PLMN entry.

clear epdg-service statistics

Use the following CLI commands to clear the PLMN based statistics for all PLMNs in ePDG service.

```
clear epdg-service statistics  plmn all
clear epdg-service statistics  mcc mcc_value mnc mnc_value
```

Notes:

- **clear epdg-service statistics**: Clears ePDG service-related statistical information.
- **plmn**: Clears ePDG service-related statistical information at PLMN.
- **all**: Clears the PLMN level statistics for all the PLMNs.
- **mcc**: Clears the PLMN level statistics for this MCC followed by MNC of PLMN.*mcc_value* allows you to enter a number, ranging from 100 to 999.
- **mnc**: Clears the PLMN level statistics for this MNC. *mnc_value* allows you to enter a number, ranging from 00 to 999.

Configuring epdg-plmn schema

Use the following CLI commands to create new bulkstats schema for PLMN level statistics.

```
configure
   bulkstats collection
   bulkstats mode
      [no] epdg-plmn schema SchemaEPDGPlmn1 format format_string active-only
format format_string
  end
```

NOTES:

- **epdg-plmn schema format** *format_string* **active-only**: Configures ePDG-PLMN bulk statistic schema.
- **schema** *schema_name* : Enter string of size 1 to 31.

- **format** *format_string* : Designates naming convention format to use.Enter string of size 1 to 3599.
- **active-only**: Gathers statistics on active chassis only.
- **no** : Deletes bulkstats schema for PLMN level statistics.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show epdg-service name

The outputs of the **show epdg-service name** *epdg_service_name* command displays the following details.

Field	Description
Service name	
Associated PLMN List	Displays the associated PLMN list for a specified ePDG service.

show plmn-list summary

The output of the **show plmn-list summary**command displays all the PLMN lists configured on the system.

Field	Description
Plmn-list	Displays the configured PLMN list name.
context	Displays the context name in which PLMN list is defined.

show epdg-service statistics plmn mcc mcc_value mnc mnc_value

The following table lists the output of **show epdg-service statistics plmn mcc mcc_value mnc mnc_value** command.

Field	Description
ePDG PLMN Statistics	
Setup attempts	Total number of setup attempts.
Setup Success	Total number of setup succeded.
Setup Failures	Total number of setup failed.
Active GTP UE	Total number of active GTP User equipments in the system.

Field	Description
Total Sessions	Total number of active sessions.
Handoff Sessions	Total number of successful handoff sessions.
ePDG To PGW Fallback	
Attempt	Total number of P-GW Fallback sessions attempted.
Success	Total number of P-GW Fallback sessions succeeded.
LTE to Wifi Handoff	
Attempt	Total number of LTE to Wi-Fi handoff attempted/
Success	Total number of sucessful LTE to Wi-Fi handoff sessions.
ePDG Reauthorisation	
Attempt	Total number of reauthorization attempted messages.
Success	Total number of successful ePDG reauthorization messages.
Session Disconnect reason	
Remote disconnect	Total number of Remote disconnected sessions.
Admin disconnect	Total number of Admin disconnected sessions.
Idle timeout	Total number of session disconnects due to idle timeout.
Absolute timeout	Total number of session disconnects due to abosolute timeout.
Long Duration timeout	Total number of session disconnects due to long duration timeout.
Session setup timeout	Total number of session disconnects due to setup timeout.
No resource	Total number of session disconnects due to non-availability of resources.
Auth failure	Total number of session disconnects due to authentication failure.
Flow add failure	Total number of session disconnects due to flow add failure.
Invalid dest-context	Total number of session disconnects due to invalid destination context.
Source address violation	Total number of session disconnects due to source address violation.
LMA Revocations (non-HO)	Total number of session disconnects due to LMA revocation.
Duplicate Request	Total number of session disconnects due to duplicate requests.
Addr assign failure	Total number of session disconnects due to address assignation failure.

Field	Description
LTE/Other handoff	Total number of session disconnects due to LTE and other handoff reasons.
Miscellaneous reasons	Total number of session disconnects due to miscellaneous reasons.
EAP Server Stats:	
Pass through mode:	
Total Msgs Received	Shows total number of EAP server messages received on pass through mode.
Success Received	Shows total number of successful EAP server messages received on pass through mode.
Diameter Authentication Statistics	
DER TX	Total number of DER messages transmitted.
DEA Challenge RX	Total number of DEA Challenge messages received.
DEA Accept RX	Total number of DEA Accept messages received.
RAR RX	Total number of RAR messages received.
RAA TX	Total number of RAA messages transmitted.
ASR RX	Total number of ASR messages received.
ASA TX	Total number of ASA messages transmitted.
STR TX	Total number of STR messages transmitted.
STA RX	Total number of STA messages received.
S2b Statistics	
GTP Attempts	.Total number of GTP attempts.
GTP Success	Total number of successful GTP sessions.
GTP Failures	Total number of failed GTP sessions.
Create Bearer Request RX	Total number of Create Bearer Request messages received.
Create Bearer Response Accepted TX	Total number of Create Bearer Response Accepted messages transmitted.
Create Bearer Request Discarded RX	Total number of Create Bearer Request Discarded messages received.
Create Bearer Response TX	Total number of Create Bearer Response transmitted.
Create Bearer Response Denied TX	Total number of Create Bearer Response Denied messages transmitted.

Field	Description
Delete Session Request TX	Total number of Delete session requests transmitted.
Delete Session Response Accepted RX	Total number of Delete session response accepted messages received.
Delete Bearer Request RX	Total number of Delete Bearer Request messages received.
Delete Bearer Response Accepted TX	Total number of Delete Bearer Response Accepted messages transmitted.
SWu Stats	
Phase 1 Auth Success	Total number of IKEv2 authentication phase 1success messages.
Phase 1 Auth Failure	Total number of IKEv2 authentication phase 1 failure messages.
Phase 1 Auth Req Sent	Total number of IKEv2 authentication phase 1 requests sent.
Total IKEA SA Deletes	
Req Sent	Total number of IKE SA delete requests sent.
Rsp Rcvd	Total number of IKE SA delete responses received.

Bulk Statistics

The following bulk statistics are added to the epdg-plmn schema:

show bulkstats variables ePDG-plmn

The following PLMN level statistics are added for the existing system level statistics.

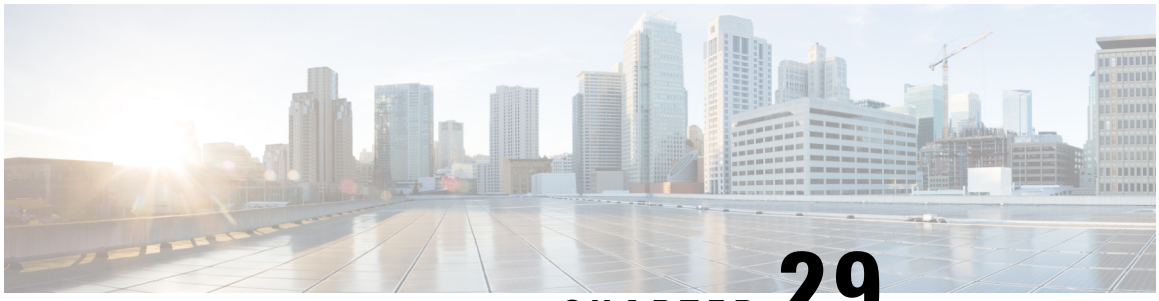
Variables	Description
plmn-mcc	The PLMN MCC for which this statistic is collected. This is a key variable.
plmn-mnc	The PLMN MNC for which this statistic is collected. This is a key variable.
ePDG Service	
plmn-totsetup-success	Displays the total number of initial attach success setups of ePDG services. **Type:** Counter
plmn-tot-success-handoff	Displays the total number of successful LTE to Wifi handoffs.
plmn-tot-handoff-attempts	Displays the total number of LTE to Wifi handoff attempts.

Variables	Description
plmn-totsetup-attempt	Displays the total number of ePDG setup sessions attempted.
plmn-totattempt-failure	Displays the total number of failure attempts of ePDG setup.
plmn-totgtp-curr-ue-in-sys	Displays the total GTP active UEs in the system.
plmn-curses	Displays the total number of current ePDG sessions.
plmn-tot-success-handoff	Displays the total number of successful handoff sessions.
plmn-pgw-fallback-succeeded	Displays the total number of P-GW Fallback sessions succeeded.
plmn-pgw-fallback-attempted	Displays the total number of P-GW Fallback sessions attempted.
plmn-reauthor-success	Displays the total number of successful reauthorization.
plmn-reauthor-attempt	Displays the total number of reauthorization attempted.
plmn-eap-rxsuccsrvrpassthru	Displays the total number of EAP-Success messages received from the EAP server in pass-through mode.
plmn-eap-rxttlsrvrpassthru	Displays the total number of EAP messages received from the EAP server in pass-through mode.
plmn-sess-disconnect-remote	Displays the total number of Remote disconnect sessions.
plmn-sess-disconnect-admin	Displays the total number of Administrator disconnect sessions at PLMN level.
plmn-sess-disconnect-idle-timeout	Displays the total number of disconnect sessions due to idle timeout reasons.
plmn-sess-disconnect-abs-timeout	Displays the total number of disconnect sessions due to absolute timeout reasons.
plmn-sess-disconnect-longdur-timeout	Displays the total number of disconnect sessions due to long duration timeout.
plmn-sess-disconnect-sesssetup-timeout	Displays the total number of sessions disconnects due to setup timeout.
plmn-sess-disconnect-noresource	Displays total number of sessions disconnects due to nonavailability of resources.

Variables	Description
plmn-sess-disconnect-authfail	Displays the total number of session disconnects due to authentication failure.
plmn-sess-disconnect-flowadd-failure	Displays the total number of session disconnects due to flow add failure.
plmn-sess-disconnect-invalid-dest	Displays the total number of session disconnects due to invalid destination context.
plmn-sess-disconnect-srcaddr-violation	Displays the total number of session disconnects due to source address violation.
plmn-sess-disconnect-lmarevoc	Displays the total number of session disconnects due to LMA revocation.
plmn-sess-disconnect-dupreq	Displays the total number of sessions disconnects due to duplicate requests.
plmn-sess-disconnect-addrassign-failure	Displays the total number of sessions disconnects due to address assignation failure.
plmn-sess-disconnect-handoff	Displays the total number of sessions disconnects due to LTE and other handoff reasons.
plmn-sess-disconnect-misc	Displays the total number of sessions disconnects due to miscellaneous reasons.
SWu Stats	
plmn-ikev2-auth-p1req	Displays the total number of IKEv2 authentication phase 1 request messages.
plmn-ikev2-auth-p1succ	Displays the total number of IKEv2 authentication phase 1 success messages.
plmn-ikev2-auth-p1fail	Displays the total number of IKEv2 authentication phase 1 failure messages.
plmn-ikev2-ikesadelrep-recv	Displays the total number of IKEv2 SA delete request received.
plmn-ikev2-ikesadelrep-sent	Displays the total number of IKEv2 SA delete requests sent.
Diameter Authentication Statistics	
plmn-der-req-id-sent	Displays the total number of DER messages transmitted.
plmn-dea-chal-rcvd	Displays the total number of DEA Challenge messages received.

Variables	Description
plmn-dea-acpt-rcvd	Displays the total number of DEA Accept messages received.
plmn-diamauth-msg-rar	Displays total number of RAR messages received.
plmn-diamauth-msg-raa	Displays the total number of RAA messages transmitted.
plmn-diamauth-msg-asr	Displays the total number of ASR messages received.
plmn-diamauth-msg-asa	Displays the total number of ASA messages transmitted.
plmn-diamauth-msg-str	Displays the total number of STR messages transmitted.
plmn-diamauth-msg-sta	Displays the total number of STA messages received.
S2b Statistics	
plmn-totgtp-attempt	Displays the total number of GTP attempts on S2b interface.
plmn-totgtp-success	Displays the total number of successful GTP sessions on S2b interface.
plmn-totgtp-failure	Displays the total number of failed GTP sessions.
plmn-tun-recv-crebear	Displays the total number of Create Bearer Request messages received.
plmn-tun-sent-crebearrespaccept	Displays the total number of Create Bearer Response Accepted messages transmitted.
plmn-tun-recv-crebearDiscard	Displays the total number of Create Bearer Request Discarded messages received.
plmn-tun-sent-crebearres	Displays the total number of Create Bearer Responses transmitted.
plmn-tun-sent-crebearrespdenied	Displays the total number of Create Bearer Response Denied messages transmitted.
plmn-tun-sent-delsessreq	Displays the total number of Delete session requests transmitted.
plmn-tun-recv-delsessrespaccept	Displays the total number of Delete session responses accepted messages received.
plmn-tun-recv-delbearreq	Displays the total number of Delete Bearer Request messages received.

Variables	Description
plmn-tun-sent-delbearrespaccept	Displays the total number of Delete Bearer Response messages transmitted.



CHAPTER 29

PLMN Level Statistics for SaMOG Services

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SaMOG
Applicable Platform(s)	• ASR 5500 • ASR 5700 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	• *SaMOG Administration Guide* • *Command Line Interface Reference* • *Statistics and Counters Reference Guide*

Revision History

Revision Details	Release
In this release, SaMOG supports PLMN level statistics for Samog services.	21.23

Feature Description

The SaMOG level statistics that are available at the SaMOG system level does not allow operators pin-point issues to certain users of the network. PLMN-based statistics is captured and displayed in the CLI and bulk statistics to help operators localize failures to a particular circle. The PLMN-based statistics allows operators to decide on the load that is generated on the SaMOG from different circles and helps in network planning.

- SaMOG extracts the PLMN information, such as Mobile Country Code (MCC) and Mobile Network Code (MNC) from International Mobile Subscriber Identity (IMSI) received in the Radius Access Request message.
- SaMOG associates PLMN list to samog-services to enable the collection of PLMN level statistics for all the PLMN's present in the list.
- Displays PLMN statistics in CLI through mandatory options of MCC and MNC.
- Facility to clear the PLMN-based statistics for all PLMNs and for a specific PLMN based on MCC and MNC.
- The PLMN statistics is applicable only for the combination of RADIUS Access-Request based triggers, EoGRE user-plane, Diameter-based authentication with AAA on STa interface and GTPv2 based S2A interface.
- Displays PLMN level statistics of all the PLMNs in the **samog-plmn schema** bulk statistics.

Configuring PLMN-list

Use the following PLMN list command to capture the statistics at PLMN level. PLMN level statistics will be captured, only if the IMSI received during initial attach / Handoff belongs to one of the PLMNs in the associated PLMN list. By default no PLMN list is configured.

```
configure
  context context_name
    plmn-list plmn_list_name
      mcc mcc_value  mnc mnc_value
      end
```

- **plmn-list**: Configures a list of PLMNs (MCC and MNC) and association to samog-service is required for capturing PLMN level statistics. A maximum of 25 PLMNs are allowed in a list. You can create a maximum of 10 PLMN lists for each context.
- **plmn_list_name**: Enter a name of size 1 to 63
- **mcc** *mcc_value*: Configures the PLMN MCC in the PLMN list. Enter a number, ranging from 100 to 999.

- **mnc** *mnc_value*: Configures the PLMN MNC in the PLMN list. Enter a number, ranging from 00 to 999.

Note List of MCCs with 3 digit MNCs are:

300 302 310 311 312 313 316 334 338 342 344 346 348 354 356 358 360 365 376 405 708 722 732

If you enter MCC, which is present in the above list, then MNC shall be of 3 digits. If you enter a 2-digit MNC for this case, then '0' shall be prefixed to it and stored in the memory. When "show plmn-list name plmn-name" command is executed, then MNC with prefixed '0' is displayed in the output.

Similarly, if user enters MCC which is NOT present in the above list, then MNC shall be of 2 digits. If user enters a 3-digit MNC for this case (with '0' prefixed), then the prefixed '0' shall be removed and stored in the memory. When "show plmn-list name plmn-name" command is executed, then MNC without prefixed '0' is displayed in the output. If the entered MNC is more than 99, then error message is displayed.

For all other combinations, it shall be stored and displayed as it is.

Associate PLMN List to SaMOG Services

Use the following command to associate the PLMN List with the SaMOG service.

```
configure
  context context_name
    samog-service service_name
      [ no ] associate plmn-list  plmn_value
      end
```

Notes:

- **associate plmn-list** *plmn_value* : Associates PLMN list with SaMOG services.
- **no**: Dis-associates the PLMN List with SaMOG service and clears the existing PLMN statistics, if present for that PLMN

Removing PLMN List Configuration

Use the following command to remove the PLMN list. This command stops SaMOG or ePDG from capturing the statistics at PLMN level and clears the existing PLMN statistics if present for that PLMN.

```
configure
  context  context_name
    no plmn-list   plmn_name
    end
```

NOTES:

- **no plmn-list** *plmn_name* : Removes the PLMN list and stops the PLMN level statistics collection for that PLMN.

Add or Remove PLMN to or from PLMN list

Use the following command to add or remove PLMN to/from PLMN list.

```
configure
   context  context_name
      plmn-list   plmn_name
          no  mcc   mcc_value mnc mnc_value
          end
```

NOTES:

- **no mcc mnc**: Removes PLMN entry with MCC and MNC combination from PLMN list. This commnad clears existing statistics if present for that PLMN.
- **mcc** *mcc_value* **mnc** *mnc_value*: Adds or removes the PLMN entry.

Configuring samog-plmn schema

Use the following CLI commands to create new bulkstats schema for PLMN level statistics.

```
configure
   bulkstats mode
     [ no ] samog-plmn schema  schema_name [ active-only ] format format_string

     end
```

- **samog-plmn schema** : Configures SaMOG-PLMN bulk statistic schema.

  schema_name alllows you to enter a string of size 1 to 31.
- **active-only**: Gathers statistics on active chassis only.
- **format** *format_string* : Designates naming convention format to use. Enter string of size 1 to 3599.
- **no** : Deletes bulkstats schema for PLMN level statistics.

clear samog-service statistics

Use the following CLI commands to clear the PLMN based counters in SaMOG service for all the PLMNs or to a particular PLMN.

```
clear samog-service statistics  plmn all
         clear samog-service statistics  mcc mcc_value mnc mnc_value
         end
```

Notes:

- **clear samog-service statistics**: Clears SAMOG service-related statistical information.
- **plmn**: Clears SAMOG service-related statistical information at PLMN.
- **all**: Clears the PLMN level statistics for all the PLMNs.
- **mcc**: Clears the PLMN level statistics for this MCC followed by MNC of PLMN.*mcc_value* allows you to enter a number, ranging from 100 to 999.

- **mnc**: Clears the PLMN level statistics for this MNC.*mnc_value* allows you to enter a number, ranging from 00 to 999.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show plmn-list name

The output of the **show plmn-list name <plmnn1>** command displays the following details:

Table 24:

Field	Description
PLMN List Context	Displays the context name under which the PLMN list is configured.
PLMN List name	Displays the name of the PLMN list.
PLMN Count in List	Displays the number of PLMNs configured in the PLMN list.
PLMN Details	Displays the MCC and MNC of the PLMNs configured in the PLMN list.

show plmn-list summary

The output of the **show plmn-list summary** command displays the following details.

Table 25:

Field	Description
Plmn-list	Displays the details of all the plmn lists configured .
context	Displays the associated PLMN list for a specified SaMOG service.

show samog-service name

The outputs of the **show samog-service name <samog1>** command displays the following new row is added.

Table 26:

Field	Description
Service name	

Field	Description
Associated PLMN List	Displays the associated PLMN list for a specified SaMOG service.

show samog-service Statistics

show samog-service statistics plmn mcc <mcc1> mnc <mnc1>

The following table lists the output of **show samog-service statistics plmn mcc <mcc1> mnc <mnc1>** command.

Table 27:

Field	Description
PLMN Level Statistics	
Active GTPv2 PDNs	Total number of active GTPv2 PDN sessions received.
GTPv2 Sessions	Total number of GTPv2 sessions received.
EAP Session Statistics	
Attempted	Total number of EAP sessions attempted.
Success	Total number of EAP sessions succeeded.
Failure	Total number of failed EAP sessions.
Current	Total number of active EAP sessions.
S2A Statistics	
Create Session Request TX	Total number of Create Session Request sessions transmitted on S2A interface.
Create Session Response Accept RX	Total number of Create Session Response Accept messages received based on S2A interface.
Create Bearer Request RX	Total number of Create Bearer Request messages received.
Create Bearer Response Accept TX	Total number of Create Bearer Response Accept messages transmitted.
Delete Session Request TX	Total number of Delete session requests transmitted.
Delete Session Response Accept RX	Total number of Delete session responses received.
Delete Bearer Request RX	Total number of Delete Bearer request messages received.
Delete Bearer Response Accept TX	Total number of Delete Bearer response messages transmitted.
Diameter Authentication Statistics	
DER TX	Total number of DER messages transmitted.

Field	Description
DEA Accept RX	Total number of DEA Accept messages received.
DEA Challenge Received"	Total number of DEA Challenge messages received.
RAR RX	Total number of RAR messages received.
RAA TX	Total number of RAA messages transmitted.
ASR RX	Total number of ASR messages received.
ASA TX	Total number of ASA messages transmitted.
STR TX	Total number of STR messages transmitted.
STA RX	Total number of STA messages received.
DHCPv6 Statistics	
IPV6 RA TX	Total number of IPV6 RA messages transmitted.
DHCP Statistics	
DHCP Sessions Active	Total number of active DHCP sessions.
DHCP Sessions Setup	Total number of DHCP sessions that are created.
DHCP Sessions Released	Total number of DHCP sessions released.
DHCP DISCOVER RX	Total numbers of DHCP discover messages received.
DHCP OFFER TX	Total number of DHCP offer messages transmitted.
DHCP REQUEST RX	Total number of DHCP request messages received.
DHCP ACK TX	Total number of DHCP acknowledgment messages transmitted.
DHCP NAK TX	Total number of DHCP NAK messages transmitted.
RADIUS Accounting Statistics	
Accounting-Request TX	Total number of RADIUS accounting request DHCP messages transmitted.
Accounting-Response RX	Total number of RADIUS accounting response messages received..
Accounting-Start TX	Total number of RADIUS accounting start messages transmitted.
Accounting-Stop TX	Total number of RADIUS accounting stop messages transmitted.
Accounting-Request Timeout	Total number of RADIUS accounting request messages that are timed out.

show bulkstats variables samog-plmn

The following PLMN level statistic variables are added for the existing system level statistics.

Table 28: Bulk Statistic Variables in the SaMOG-plmn Schema

Variables	Description	Data Type
plmn-mcc	**Description:** The MCC of the PLMN received in IMSI. This is a key variable. **Type:** Information	Int16
plmn-mnc	**Description:** The MNC of the PLMN received in IMSI. This is a key variable **Type:** Information	String
plmn-mrme-access-mode-gtpv2-selected	**Description:** Displays the total number of sessions selected in a PLMN with network access mode as GTPv2 **Triggers**: Incremented whenever subscriber session is selected as P-GW (S2a over GTPv2) . **Type:** Counter	Int32
plmn-mrme-eap-call-attempted	**Description:** Displays the total number of MRME EAP Sessions Attempted. **Triggers**: Increments whenever a EAP session establishment is attempted at PLMN level. **Type:** Counter	Int32
plmn-mrme-eap-call-success	**Description:** Displays the total number EAP sessions sunccessfully established at PLMN level. **Triggers**: Increments whenever a EAP session establishment is successful at PLMN level. **Type:** Counter	Int32
plmn-mrme-eap-call-failure	**Description:** Displays the total number of EAP sessions that failed to be created at PLMN level. **Triggers**: Incremented whenever a EAP session establishment fails at PLMN level. **Type:** Counter	Int32

Variables	Description	Data Type
plmn-mrme-eap-call-current	**Description:** Displays the total number of EAP sessions currently established at PLMN level. **Triggers**: Incremented whenever a EAP session establishment is successful and decrements when session is deleted at PLMN level. **Type:** Gauge	Int32
plmn-cgw-sessstat-pdns-gtpv2-active	**Description:** Displays the total number of current active GTPV2 PDN connections at PLMN level. **Triggers**: Incremented whenever a GTPv2 connection is created by SaMOG and decrements whenever GTPV2 DN connection is released by SaMOG at PLMN level. **Type:** Gauge	Int32
plmn-dhcp-curservsess	**Description:** Displays the total number of DHCP service sessions active on the system at PLMN level. **Type:** Gauge	Int32
plmn-sess-total-setup	**Description:** Displays the total number of DHCP setup sessions at PLMN level. **Type:** Counter	Int32
plmn-total-released	**Description:** Displays the total number of DHCP sessions released at PLMN level. **Type:** Counter	Int32
plmn-dhcp-msg-discover-rx	**Description:** Displays the total number of DHCP discover messages received at PLMN level. **Type:** Counter	Int32
plmn-dhcp-msg-offer-tx	**Description:** Displays the total number of DHCP offer messages transmitted at PLMN level. **Type:** Counter	Int32
plmn-dhcp-msg-request-rx	**Description:** Displays the total number of DHCP request messages received at PLMN level. **Type:** Counter	Int32

Variables	Description	Data Type
plmn-dhcp-msg-ack-tx	**Description:** Displays the total number of DHCP acknowledgement messages transmitted at PLMN level. **Type:** Counter	Int32
plmn-dhcp-msg-nak-tx	**Description:** Displays the total number of transmitted DHCP nessages that are not acknowledged. **Type:** Counter	Int32
plmn-cgw-sessstat-ipv6-router-advt-sent	**Description:** Displays the total number of router advertisement messages received at PLMN level. **Triggers**: Incremented whenever router advertisement messages is sent for sessions at PLMN level. **Type:** Counter	Int32
plmn-tun-sent-cresess	**Description:** Displays the total number of initial tunnel-create session request message sent by the system at PLMN level. **Triggers**: Incremented whenever initial tunnel-create session request message is sent by the system at PLMN level. **Type:** Counter	Int32
plmn-tun-recv-cresessrespaccept	**Description:** Displays the total number of tunnel-create-session response accepted messages received by the systme at PLMN level. **Triggers**: Incremented whenever create-session-response accepted message is received by the system at PLMN level. **Type:** Counter	Int32
plmn-tun-recv-crebear	**Description:** Displays the total number tunnel-create bearer request message is received by the system at PLMN level. **Triggers**: Incremented whenever create bearer sesion response accepted messages is received by the system at PLMN level. **Type:** Counter	Int32

Variables	Description	Data Type
plmn-tun-sent-crebearrespaccept	**Description:** Displays the total number of tunnel-create-bearer-response accepted message sent by the system at PLMN level. **Triggers**: Incremented whenever create bearer response accepted messages is sent by the system at PLMN level. **Type:** Counter	Int32
plmn-tun-sent-delsessreq	**Description:** Displays the total number of tunnel-delete-session-response-accepted messages received by the system at PLMN level. **Type:** Counter	Int32
plmn-tun-recv-delsessrespaccept	**Description:** Displays the total number of tunnel-delete-bearer-response-accepted messages sent by the system at PLMN level. **Triggers**: Incremented whenever delete bearer response messages with accepted cause is sent by the system at PLMN level. **Type:** Counter	Int32
plmn-tun-recv-delbearreq	**Description:** Displays the total number of Delete Bearer Request Initial messages received. **Type:** Counter	Int32
plmn-tun-sent-delbearrespaccept	**Description:** Displays the total number of Delete Bearer Response Accepted messages transmitted. **Type:** Counter	Int32
plmn-der-req-id-sent	**Description:** Displays the total number of Diameter-EAP-Request (DER) messages sent at PLMN level. **Triggers**: Incremented whenever a DER message is sent at PLMN level. **Type:** Counter	Int32

Variables	Description	Data Type
plmn-dea-chal-rcvd	**Description:** Displays the total number of DEA Challenge messages received at PLMN level. **Triggers**: Incremented whenever a DEA message is receivedent with EAP challenge at PLMN level. **Type:** Counter	Int32
plmn-dea-acpt-rcvd	**Description:** Displays the total number of DEA Accept messages received at PLMN level. **Triggers**: Incremented whenever a DEA is received with Result-code value as 2001 at PLMN level. **Type:** Counter	Int32
plmn-diamauth-msg-asr	**Description:** Displays the total number of Abort-Session_Request messages received at PLMN level. **Triggers**: Incremented whenever an ASR received at PLMN level. **Type:** Counter	Int32
plmn-diamauth-msg-asa	**Description**:Displays the total number of Abort-Session-Answer-sent at PLMN level. **Triggers**: Incremented whenever an ASA is sent at PLMN level. **Type:** Counter	Int32
plmn-diamauth-msg-rar	**Description**: Displays the total number of Re-Auth-Request messages received at PLMN level. **Triggers**: Incremented whenever an RAR is received at PLMN level. **Type:** Counter	Int32
plmn-diamauth-msg-raa	**Description**: Displays the total number of Re-Auth-Answer messages sent at PLMN level. **Triggers**: Incremented whenever an RAA is sent at PLMN level. **Type:** Counter	Int32

Variables	Description	Data Type
plmn-diamauth-msg-str	**Description**:Displays the total number of Session-Termination-Request (STR) messages sent at PLMN level. **Triggers**: Incremented whenever an STR is sent at PLMN level. **Type:** Counter	Int32
plmn-diamauth-msg-sta	**Description**: Displays the total number of Session-Termination-Answer (STA) messages received at PLMN level. **Triggers**: Incremented whenever an STA is received at PLMN level. **Type:** Counter	Int32
plmn-acc-req-sent	**Description**: Displays the total number of Accounting requests sent to the server at PLMN level. **Triggers**: Incremented whenever an Accounting requests sent to the RADIUS server at PLMN level. **Type:** Counter	Int32
plmn-acc-rsp-rcvd	**Description**: Displays the total number of Accounting responses received from the server at PLMN level. **Triggers**: Incremented whenever an Accounting responses is received from RADIUS server at PLMN level. **Type:** Gauge	Int32
plmn-acc-start-sent	**Description:** Displays the total number of Accounting Start messages sent at PLMN level. **Triggers**: Incremented whenever an Accounting Start messages is sent at PLMN level. **Type:** Counter	Int32

Variables	Description	Data Type
plmn-acc-stop-sent	**Description:** Displays the total number of Accounting Stop messages sent at PLMN level. **Triggers**: Incremented whenever an Accounting Stop messages is sent at PLMN level. **Type:** Counter	Int32
plmn-acc-req-timeout	**Description:** Displays the total number of Accounting requests timed out at PLMN level. **Triggers**: Incremented whenever an Accounting requests timed out at PLMN level. **Type:** Counter	Int32

Bulk Statistics

The following bulk statistics are added to the epdg-plmn schema:

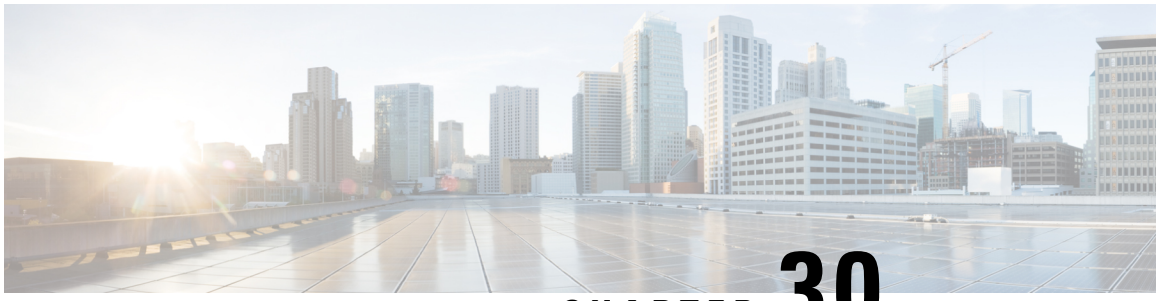
samog-plmn-schema

Table 29: Bulk Statistics Variables in the SaMOG-plmn Schema

Variables	Description
plmn-mcc	The PLMN MCC context configured at the PLMN level that is currently facilitating the SaMOG Service. This is a key variable.
plmn-mnc	The PLMN MNC context configured at the PLMN level that is currently facilitating the SaMOG service. This is a key variable.
plmn-mrme-access-mode-gtpv2-selected	Indicates that the Network access mode statistics for the selected gtpv2 interface.
plmn-mrme-eap-call-attempted	Indicates that the total number of MRME EAP Session Attempted.
plmn-mrme-eap-call-success	Indicates that the total number of successful MRME EAP sessions.
plmn-mrme-eap-call-failure	Indicates that the total number of failed MRME EAP sessions.
plmn-mrme-eap-call-current	Indicates that the total number of current MRME EAP sessions.
plmn-cgw-sessstat-pdns-gtpv2-active	Indicates that the total number of session statistics active for PDN gtpv2 interface.
plmn-dhcp-curservsess	Indicates that the total number of DHCP server sessions that are active.

Variables	Description
plmn-sess-total-setup	Indicates that the total number of DHCP Sessions setup.
plmn-total-released	Indicates that the total number of DHCP sessions released.
plmn-dhcp-msg-discover-rx	Indicates that the total number of DHCP discover messages received.
plmn-dhcp-msg-offer-tx	Indicates that the total number of DHCP offer messages transmitted.
plmn-dhcp-msg-request-rx	Indicates that the total number of DHCP request messages received.
plmn-dhcp-msg-ack-tx	Indicates that the total number of DHCP acknowledgment messages transmitted.
plmn-dhcp-msg-nak-tx	Indicates that the total number of transmitted DHCP messages that are not acknowledged.
plmn-cgw-sessstat-ipv6-router-advt-sent	Indicates that the total number of router advertisement messages sent.
plmn-tun-sent-cresess	Indicates the total number of Create Sessions Request Initially transmitted.
plmn-tun-recv-cresessrespaccept	Indicates that the total number of Create Session Response Accepted messages received.
plmn-tun-recv-crebear	Indicates that the total number of Create Bearer Requests Initial messages received.
plmn-tun-sent-crebearrespaccept	Indicates that the total number of Create Bearer Response Accepted messages transmitted.
plmn-tun-sent-delsessreq	Indicates that the total number of Delete Session Request Initial messages transmitted.
plmn-tun-recv-delsessrespaccept	Indicates that the total number of Delete Session Response Accepted messages received.
plmn-tun-recv-delbearreq	Indicates that the total number of Delete Bearer Request Initial messages received.
plmn-tun-sent-delbearrespaccept	Indicates that the total number of Delete Bearer Response Accepted messages transmitted.
plmn-der-req-id-sent	Indicates the total number of DE Requests.
plmn-dea-chal-rcvd	Indicates that the total number of DEA Challenge statistics received.
plmn-dea-acpt-rcvd	Indicates that the total number of DEA Accept statistics received.

Variables	Description
plmn-diamauth-msg-asr	Indicates that the total number of Diameter authentication messages are received for ASR.
plmn-diamauth-msg-asa	Indicates the total number of Diameter authentication messages received for ASA.
plmn-diamauth-msg-rar	Indicates the total number of Diameter authentication messages received for RAR.
plmn-diamauth-msg-raa	Indicates that the total number of Diameter authentication messages for RAA
plmn-diamauth-msg-str	Indicates that the total number of Diameter authentication messages are received for STR.
plmn-diamauth-msg-sta	Indicates that the total number of Diameter authentication messages are received for STA.
plmn-acc-req-sent	Indicates that the total number of PLMN accounting requests sent.
plmn-acc-rsp-rcvd	Indicates that the total number of PLMN accounting responses are received.
plmn-acc-start-sent	Indicates that the total number of PLMN accounting start messages are sent.
plmn-acc-stop-sent	Indicates that the total number of PLMN accounting stop messages sent.
plmn-acc-req-timeout	Indicates that the total number of PLMN accounting requests timed out.



CHAPTER 30

Separation of 2G 3G 4G WLAN Bulkstatistics

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-GW • SAEGW
Applicable Platform(s)	All
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

Revision History

Revision Details	Release
In this release, separation of 2G 3G 4G WLAN Bulk Statistics is introduced	21.23
First introduced.	21.5

Feature Description

Some of the contractual Key Performance Indicators (KPIs) are monitored by operations that require reporting per Radio Access Technology (RAT) type (2G, 3G, 4G). A few of the bulkstat counters implemented currently do not separate the RAT type. To enable and disable per APN RAT types statistics, the newly introduced RAT types are"gtpv2-s2a" and "gtpv2-s2b".These types provide RAT separation (2G, 3G, 4G, WLAN).

This separation enables the operations team to report the usage by RAT type separately, as well as enhance the troubleshooting tools used to detect any network issues.

Configuring RAT types in Stats Profile

The configuration command gtpv2-s2a and gtpv2-s2b has been added to the stats-profile configuration mode. It integrates the per APN per RAT type (2G, 3G, 4G, gtpv2-s2a, gtpv2-s2b) statistics with the existing stats-profile implementation.

To enable per APN per RAT types statistics collection, execute the following command:

```
configure
  stats-profile stats_profile_name
    [ no ]  rat-type { gtpv2-s2a | gtpv2-s2b }
  end
```

After the association of stats-profile with APN, the statistics are collected for and this requires APN per RAT level statistics.

Per APN per RAT level statistics are lost if stats-profile association is removed from APN and RAT type option is removed from stats-profile.

To assoicate stats-profile with APN , execute the following command:

```
configure
  context context_name
    apn apn_name
      stats-profile stats_profile_name
  end
```

NOTES:

- **stats-profile** : Configures statistics profile to collect packet drop counters and/or ARP level stats.
- **rat-type** Configures collection of RAT level statistics.
- **gtpv2-s2a** Configures collection of statistics for RAT Type WLAN S2A.
- **gtpv2-s2b** Configures collection of statistics for RAT Type WLAN S2B.

Monitoring and Troubleshooting

This section provides information on the show commands and bulk statistics available to support the 2G, 3G, 4G, WLAN bulkstat separation.

Show Command and Output

show stats-profile all

The output of this command displays the collection of statistics for RAT Type gtpv2-S2A and gtpv2-S2B as follows:

- stats profile name
- RAT Type
- gtpv2-s2a
- gtpv2-s2b

show apn statistics all

The output of this command displays the statistics of dynamic address allocation, uplink and downlink of gtpv2-s2a and gtpv2-s2b as follows:

- Data Statistics
  - gtpv2-s2a
    - Uplnk Bytes
    - Dnlnk Bytes
  - gtpv2-s2b
    - Uplnk Bytes
    - Dnlnk Bytes
- RAT Type Statistics
  - gtpv2-s2a
    - Ipv4
    - Ipv6
    - Ipv4v6
  - gtpv2-s2b
    - Ipv4
    - Ipv6

- Ipv4v6

show gtpc statistics

The output of this command displays the statictics of updated pdp context transmission and reception of GERAN and UTRAN:

- Tunnel Management Messages
  - Total GERAN Accepted
  - Total UTRAN Accepted
  - GERAN UPC RX
  - Accepted

Note The above Accepted counter is for GERAN UPC RX.

  - UTRAN UPC RX
  - Accepted

Note The above Accepted counter is for UTRAN UPC RX.

  - GERAN UPC TX
  - Accepted

Note The above Accepted counter is for GERAN UPC TX.

  - UTRAN UPC TX
  - Accepted

Note The above Accepted counter is for UTRAN UPC TX.

show gtpc statistics apn <apn_name> verbose

The output of this command displays the statistics of RAT type create pdp context statistics of GERAN and UTRAN:

- Tunnel Management Messages
  - Total GERAN Accepted

- Total UTRAN Accepted
- GERAN UPC RX
- Accepted

Note The above Accepted counter is for GERAN UPC RX.

- UTRAN UPC RX
- Accepted

Note The above Accepted counter is for UTRAN UPC RX.

- GERAN UPC TX
- Accepted

Note The above Accepted counter is for GERAN UPC TX.

- UTRAN UPC TX
- Accepted

Note The above Accepted counter is for UTRAN UPC TX.

- GERAN PDP Context Denied
  - No Resources
  - Memory
  - All Dyn Addr Occupied
  - User Auth Failed
  - Unknown Missing/APN
  - System Failure
  - Service Not Supported
  - No APN Subscription
- UTRAN PDP Context Denied
  - No Resources
  - Memory

- All Dyn Addr Occupied
- User Auth Failed
- Unknown Missing/APN
- System Failure
- Service Not Supported
- No APN Subscription

show gtpc statistics apn <apn_name>

The output of this command displays the statictics of updated pdp context transmission and reception of GERAN and UTRAN:

- Tunnel Management Messages
  - Total GERAN Accepted
  - Total UTRAN Accepted
  - GERAN UPC RX
  - Accepted

Note The above Accepted counter is for GERAN UPC RX.

  - UTRAN UPC RX
  - Accepted

Note The above Accepted counter is for UTRAN UPC RX.

  - GERAN UPC TX
  - Accepted

Note The above Accepted counter is for GERAN UPC TX.

  - UTRAN UPC TX
  - Accepted

Note The above Accepted counter is for UTRAN UPC TX.

Bulk Statistics

APN Schema

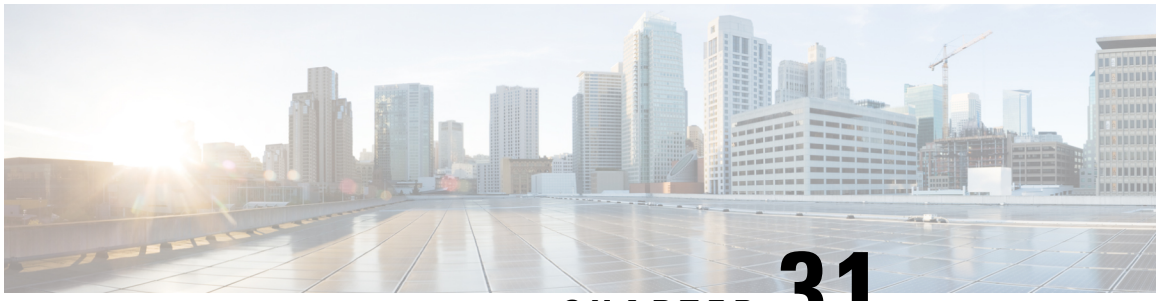
The following bulk statistics are added in the APN schema to support the 2G, 3G, 4G, WLAN bulkstats separation feature:

Bulk Statistics	Description
uplnk-bytes-gtpv2-s2a	Indicates the total number of bytes sent from the APN for a GTPV2 based S2A RAT type towards the Internet/PDN on the Gi interface.
dnlnk-bytes-gtpv2-s2a	Indicates the total number of bytes received for a GTPV2 based S2A RAT type on the Gi interface for the APN.
uplnk-bytes-gtpv2-s2b	Indicates the total number of bytes sent from the APN for a GTPV2 based S2B RAT type towards the Internet/PDN on the Gi interface.
dnlnk-bytes-gtpv2-s2b	Indicates the total number of bytes received for a GTPV2 based S2B RAT type on the Gi interface for the APN.
dyn-ipv4-success-eutran	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a EUTRAN RAT type.
dyn-ipv4-success-gtpv2-s2a	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2A RAT type.
dyn-ipv4-success-gtpv2-s2b	Indicates the total number of IPv4 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2B RAT type.
dyn-ipv6-success-eutran	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a EUTRAN RAT type.
dyn-ipv6-success-gtpv2-s2a	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2A RAT type
dyn-ipv6-success-gtpv2-s2b	Indicates the total number of IPv6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2B RAT type.
dyn-ipv4v6-success-eutran	Indicates the total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a EUTRAN RAT type.

dyn-ipv4v6-success-gtpv2-s2a	Indicates the total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2A RAT type.
dyn-ipv4v6-success-gtpv2-s2b	The total number of IPv4v6 contexts requesting dynamically assigned IP addresses that were successfully setup for a GTPV2 based S2B RAT type.
upc-rx-geran	Indicates the total number of Update PDP Context Request messages received from the SGSN(s) for a GERAN RAT type per APN.
upc-tx-geran	Indicates the total number of Update PDP Context Request messages sent to the SGSN(s) for a GERAN RAT type per APN.
upc-rx-accept-geran	Indicates the total number of Update PDP Context Response messages received from SGSN(s) containing a cause value of 128 (80H, Request accepted) for a GERAN RAT type per APN.
upc-tx-accept-geran	Indicates the total number of Update PDP Context Response messages sent to the SGSN(s) containing a cause value of 128 (80H, Request accepted) for a GERAN RAT type per APN.
upc-rx-utran	Indicates the total number of Update PDP Context Request messages received from the SGSN(s) for a UTRAN RAT type per APN.
upc-tx-utran	Indicates the total number of Update PDP Context Request messages sent to the SGSN(s) for a UTRAN RAT type per APN.
upc-rx-accept-utran	Indicates the total number of Update PDP Context Response messages received from SGSN(s) containing a cause value of 128 (80H, Request accepted) for a UTRAN RAT type per APN.
upc-tx-accept-utran	Indicates the total number of Update PDP Context Response messages sent to the SGSN(s) containing a cause value of 128 (80H, Request accepted) for a UTRAN RAT type per APN.
cpc-accept-geran	Indicates the total number of Create PDP Context Response messages transmitted containing a cause value of 128 (80H, Request accepted)for a GERAN RAT type per APN.

cpc-accept-utran	Indicates the total number of Create PDP Context Response messages transmitted containing a cause value of 128 (80H, Request accepted) for a UTRAN RAT type per APN.
cpc-nomem-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 212 (D4H, No memory is available) for a GERAN RAT type per APN.
cpc-nomem-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 212 (D4H, No memory is available) for a UTRAN RAT type per APN.
cpc-noresource-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 199 (C7H, No resources available) for a GERAN RAT type per APN.
cpc-noresource-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 199 (C7H, No resources available) for a UTRAN RAT type per APN.
cpc-srv-not-supp-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 200 (C8H, service not Supported) for a GERAN RAT type per APN.
cpc-srv-not-supp-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 200 (C8H, service not Supported) for a UTRAN RAT type per APN.
cpc-sys-fail-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 204 (CCH, System failure) for a GERAN RAT type per APN.
cpc-sys-fail-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 204 (CCH, System failure) for a UTRAN RAT type per APN.
cpc-auth-fail-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 209 for a GERAN RAT type per APN.

cpc-auth-fail-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 209 for a UTRAN RAT type per APN.
cpc-no-apn-subscription-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent for a GERAN RAT type per APN because there was no apn subscription.
cpc-no-apn-subscription-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent for a UTRAN RAT type per APN because there was no apn subscription.
cpc-missing-apn-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 219 (DBH, Missing or unknown APN) for a GERAN RAT type per APN.
cpc-missing-apn-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 219 (DBH, Missing or unknown APN) for a UTRAN RAT type per APN.
cpc-addr-occupied-geran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 211 (D3H, All dynamic PDP addresses are occupied) for a GERAN RAT type per APN.
cpc-addr-occupied-utran	Indicates the total number of reject Create PDP Context Response messages transmitted to the SGSN(s) sent with a cause code of 211 (D3H, All dynamic PDP addresses are occupied) for a UTRAN RAT type per APN.



CHAPTER 31

Secondary RAT Usage Report in CDR Records

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • SAEGW • S-GW
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* • *GTPP Interface Administration and Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
P-GW and S-GW supports secondary RAT usage reports and CDRs processing through GTPP Group Configuration CLIs.	• 21.23.14

Feature Description

Reporting issues pertaining to 5G **RANSecondaryRATUsageReport** occur due to lack of:

- Control in identifying whether the **RANSecondaryRATUsageReport** must be processed in CDRs or not. This allows the S-GW, P-GW, and SAEGW to either include these reports in the SGW-CDR or PGW- CDR or to simply ignore them.
- Number of available reports inside a CDR, if the control is active.
- Control in identifying whether Zero-volume reports must make it inside the CDR or not.

This results in billing loss of data. To overcome these reporting issues, you can trigger CLI controls using GTPP group configuration to:

- Allow the S-GW, P-GW, and SAEGW to either include the RANSecondary RAT Usage reports in the SGW-CDR or PGW-CDR or to simply ignore them.
- Identify the number of secondary RAT usage reports available inside the SGW-CDR or the PGW- CDR.

Note This limit must be in accordance with the system capability and ensure to consider the File-Format of the CDRs. If the configured limit exceeds, the system closes the SGW-CDR or PGW-CDR with the appropriate change-condition. For example, **max-change-condition** CDR is reused for further reports.

- Add or ignore Zero-volume reports inside the CDR.
- The CLI **gtpp limit-secondary-rat-usage** or hardcoded limit will be removed and the CLI **gtpp limit-secondary-rat-usage** is reused to control the number of records within the range 1-100.
- Provides logging when the CDR size reaches the maximum size. Through PGW-CDR counter, you can monitor the number of occurrences when the CDR exceeds its size limit.

Behavior Matrix

The following table explains the new behavior of P-GW and S-GW for this feature.

CLI	P-GW New Behavior	S-GW New Behavior
gtpp attribute secondary-rat-usage By default, this CLI command is enabled in gtpp group.	P-GW sends secondary RAT usage records in CDR including zero volume records.	S-GW sends secondary RAT usage records in CDR including zero volume records.
[no] gtpp attribute secondary-rat-usage	P-GW does not send secondary RAT usage records in CDR.	S-GW does not send secondary RAT usage records in CDR.
gtpp suppress-secondary-rat-usage zero-volume By default, this CLI command is disabled in gtpp group.	P-GW does not include and send zero volume secondary RAT records in CDR. P-GW sends only secondary RAT records with non-zero volumes.	S-GW does not include and send zero volume secondary RAT records in CDR. S-GW sends only secondary RAT records with non-zero volumes.
[no] gtpp suppress-secondary-rat-usage zero-volume	P-GW sends secondary RAT usage records including zero volume records in CDR.	S-GW sends secondary RAT usage records including zero volume records in CDR.
gtpp limit-secondary-rat-usage *range_1–100*. If not configured, the default value is 32. By default, this CLI command is enabled in gtpp group. **Example: gtpp limit-secondary-rat-usage 32** **Note** This CLI is the modification of the existing CLI command **gtpp limit-secondary-rat-usage** with range between 1– 100.	P-GW generates CDR immediately when total received secondary RAT records exceeds 32 and reported cause value is *maximum change condition*. P-GW generates multiple CDRs if total received secondary RAT records are multiples of 32. **Example**: If P-GW receives 100 RAT records between two triggers, P-GW generates 3 CDRs and keeps the remaining 4 RAT records for the next CDR trigger.	S-GW generates CDR immediately when total received secondary RAT records exceeds 32 and the reported cause value is *maximum change condition*. S-GW generates multiple CDRs if the total received secondary RAT records are multiples of 32. **Example**: If S-GW receives 100 RAT records between two triggers, S-GW generates 3 CDRs and keeps the remaining 4 RAT records for the next CDR trigger.
Example:gtpp limit-secondary-rat-usage 40	P-GW generates CDR immediately when total received secondary RAT records exceeds 40 and cause value is *maximum change condition*. P-GW generates multiple CDRs if total received secondary RAT records are multiples of 40. **Example**: If P-GW receives 100 RAT records between two triggers, it will generate 2 CDRs and will keep remaining 20 RAT records for the next CDR trigger.	If the configured value is greater than 32 and sends 32 secondary RAT records in every CDR, Ignores **gtpp limit-secondary-rat-usage 40** CLI command.

CLI	P-GW New Behavior	S-GW New Behavior
Example:gtpp limit-secondary-rat-usage 20	P-GW generates CDR immediately when total received secondary RAT records exceed 20 and cause value is *maximum change condition*. P-GW generates multiple CDRs if total received secondary RAT records are multiples of 20. **Example:** If P-GW receives 100 RAT records between two triggers, P-GW generates 2 CDRs and will store the remaining 20 RAT records for the next CDR trigger.	S-GW generates CDR immediately when the total received secondary RAT records exceeds 20 and cause value is *maximum change condition*. S-GW generates multiple CDRs if total received secondary RAT records are in multiples of 20. **Example**: If S-GW receives 100 RAT records between two triggers, it will generate 5 CDRs.
[no] gtpp limit-secondary-rat-usage	Generates CDR immediately when the total received secondary RAT records exceed 255 and cause value is *maximum change condition*. Generates multiple CDRs if the total received secondary RAT records are multiples of 255. **Example**: If 1000 RAT records between two triggers are received, then 3 CDRs are generated. The remaining 235 RAT records are stored for the next CDR trigger.	Ignores the **[no] gtpp limit-secondary-rat-usage** CLI and sends 32 secondary RAT records in every CDR. Behavior is similar to the **gtpp limit-secondary-rat-usage** *32* CLI implementation. Counter and debug logs are not required as it will never exceed the CDR size of 64k.
	Service-specific unit limit is sent in the **serviceConditionChange** file.	Record Closure

Relationship to Other Features

- Sessmgr Restart While Processing Secondary RAT Usage CDR Records in the *P-GW Administration Guide*.
- Secondary RAT Usage IE during GnGp handover, S-GW, and P-GW support of Secondary RAT Data Usage Report in Gz CDRs, see the *5G Non-Standalone* chapter in the *P-GW Administration Guide*.
- P-GW support of Secondary RAT Data Usage Report in Rf CDRs, see the *5G Non-Standalone* chapter in the *P-GW Administration Guide*.

Limitations

This feature has the following limitations:

- S-GW allows a maximum number of 16 secondary RAT records per bearer during session recovery and checkpointing.
- P-GW allows a maximum number of 142 secondary RAT records across all bearers during session recovery and checkpointing.
- Anything beyond these numbers gets lost during session recovery.

Configuring Secondary RAT Usage Report through GTPP

Use the following GTPP configurations to close Secondary RAT Usage CDR records before exceeding a buffer size.

Enabling or Disabling the Secondary RAT Usage Report

Use the following configuration to enable or disable secondary RAT Usage report.

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute secondary-rat-usage
      default gtpp attribute secondary-rat-usage
      no gtpp attribute secondary-rat-usage
      end
```

NOTES:

- **gtpp attribute secondary-rat-usage**: Sends an optional attribute Secondary RAT usage records.
- **default gtpp attribute secondary-rat-usage**: Sends an optional attribute Secondary RAT usage records by default.
- **no gtpp attribute secondary-rat-usage**: Does not send the optional attribute Secondary RAT usage records.

Controlling the Maximum Number of Entries

When the Secondary RAT usage record reaches the maximum configured value within a CDR, the CDR closure cause occurs and uses **maxChangeCond**. The **gtpp limit-secondary-RAT-usage** CLI command controls the maximum number of Secondary RAT usage record entries in the P-GW and S-GW CDRs. If the limit is configured with a value more than 32, the partial CDRs get generated with a maximum of 32 for S-GW CDR.

Note The existing behaviour of S-GW has a limit of 32 Secondary RAT Usage records.

The following table explains the behavior of Secondary RAT records and CDR, and the maximum limit.

Sl. Number	CDR Type	Configured limit-secondary-rat-usage	Effective Maximum Limit	No. of Secondary RAT records Sent by UE	Behavior of Secondary RAT Records and CDR
1	P-GW	Less than 32 Example: 20	20	35	Partial CDR is generated with 20 secondary RAT records.
					Remaining 15 secondary RAT records sent in the next trigger.
	S-GW	Less than 32 Example: 20	20	35	Partial CDR is generated with 20 Secondary RAT records.
					Remaining 15 Secondary RAT records sent in the next trigger.
2	P-GW	32	32	35	Partial CDR is generated with 32 Secondary RAT records.
					Remaining 3 secondary RAT records sent in the next trigger.
	S-GW	32	32	35	Partial CDR is generated with 32 secondary RAT records.
					Remaining 3 secondary RAT records sent in the next trigger.

Sl. Number	CDR Type	Configured limit-secondary-rat-usage	Effective Maximum Limit	No. of Secondary RAT records Sent by UE	Behavior of Secondary RAT Records and CDR
3	P-GW	Greater than 32 Example: 100	100	100	Partial CDR is generated with 100 secondary RAT records.
	S-GW	Greater than 32 Example: 100	32	100	Three partial CDRs are generated with 32 secondary RAT records each.
					Remaining 4 secondary RAT records sent in the next trigger.
4	P-GW	Not configured	255	1000	Three partial CDRs are generated with 255 secondary RAT records each.
					Remaining reported Secondary RAT records become a part of CDR in the next trigger.
	S-GW	Not configured	32	1000	No partial CDR is generated.
					32 Secondary RAT records become part of the CDR in the next trigger.

Use the following configuration to control the maximum number of entries.

```
configure
  context context_name
    gtpp group group_name
      gtpp limit-secondary-rat-usage usage_limit
      default gtpp limit-secondary-rat-usage
```

```
no gtpp limit-secondary-rat-usage
end
```

NOTES:

- **gtpp limit-secondary-rat-usage** *usage_limit*: Enter a maximum number of secondary RAT reports. *usage_limit* must be an integer in the range of 1-100. The recommended value for S-GW CDR is 32.

  For example, if the limit is set to 10, then the CDR is generated once the configured value is reached.

- **default gtpp limit-secondary-rat-usage**: Specifies a default value of 32.
- **no gtpp limit-secondary-rat-usage**: Disables the CDR generation with limited number of secondary RAT usage information.

Suppressing Zero-Volume Secondary RAT Usage Report

Use the following configuration to suppress zero-volume Secondary RAT Usage report.

```
configure
  context context_name
    gtpp group group_name
      gtpp suppress-secondary-rat-usage zero-volume
      default gtpp suppress-secondary-rat-usage zero-volume
      no gtpp suppress-secondary-rat-usage zero-volume
      end
```

NOTES:

- **gtpp suppress-secondary-rat-usage zero-volume**: Suppresses either Secondary RAT records or zero volume Secondary RAT records.
- **default gtpp suppress-secondary-rat-usage zero-volume**: Does not suppress the zero volume secondary RAT usage records.
- **no gtpp suppress-secondary-rat-usage zero-volume**: Does not suppress the zero volume Secondary RAT usage records.

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 config

The output of this CLI command displays the following parameters.

Field	Description
gtpp attribute secondary-rat-usage	Specify this option to include the Secondary RAT reports field in the CDR.
gtpp suppress-secondary-rat-usage zero-volume	Enables the exclusion of the zero volume Secondary RAT reports in the CDR.
gtpp limit-secondary-rat-usage	Enables limiting the number of Secondary RAT Usage reports in CDR with the configured value.

show config verbose

The output of this CLI command displays the following parameters.

Field	Description
gtpp attribute secondary-rat-usage	Displays the Secondary RAT usage records.
gtpp suppress-secondary-rat-usage zero-volume	Displays only Secondary RAT records that is having non-zero volumes from P-GW and S-GW.
gtpp limit-secondary-rat-usage	If total received Secondary RAT records are multiples of 10, displays multiple CDR generated by P-GW and S-GW. The reported cause value will be the maximum change condition.
no gtpp limit-secondary-rat-usage	Displays Secondary RAT records for unconfigured cause.

show gtpp group

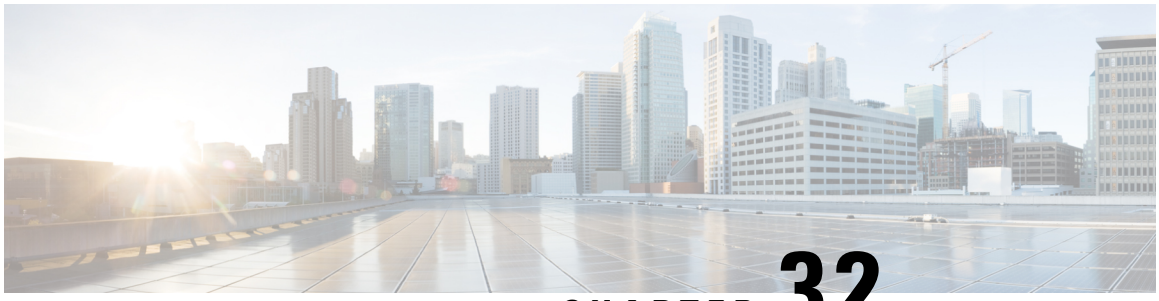
The output of this CLI command displays the following parameters.

Field	Description
Secondary RAT records present	Specifies whether the Secondary RAT record is present or not. The available options are: • no • yes
Limit-secondary-rat-usage	Specifies a limit for Secondary RAT usage report.

show gtpp statistics group

The output of this CLI command displays the following parameter.

Field	Description
Total PGW-CDR exceed size limit	Displays the total number of CDRs that exceeded size limit in P-GW.



CHAPTER 32

Sessmgr Restart While Processing Secondary RAT Usage CDR Records

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	Enabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• P-GW Administration Guide • Command Line Interface Reference

Revision History

Revision Details	Release
In this release, a new CLI command *limit-secondary-rat-usage* is introduced to limit the RAT usage report in CDR.	21.23
First Introduced	21.19.7

Feature Changes

Previous Behavior: Session Manager (SessMgr) is restarted while Charging Data Record (CDR) process is triggered. The restart occurs when the buffer reaches 64K bytes with different stacks.

New Behavior: In this and StarOS 21.23 release, the SessMgr restart can be avoided by limiting the number of Secondary Radio Access Technology (RAT) usage reports in CDR to a maximum of 32 records. A new CLI command limit-secondary-rat-usage is introduced to limit the Secondary RAT usage report in CDR.

Note By default, limit-secondary-rat-usage is disabled. This CLI is not applicable for CUSTOM38 dictionary.

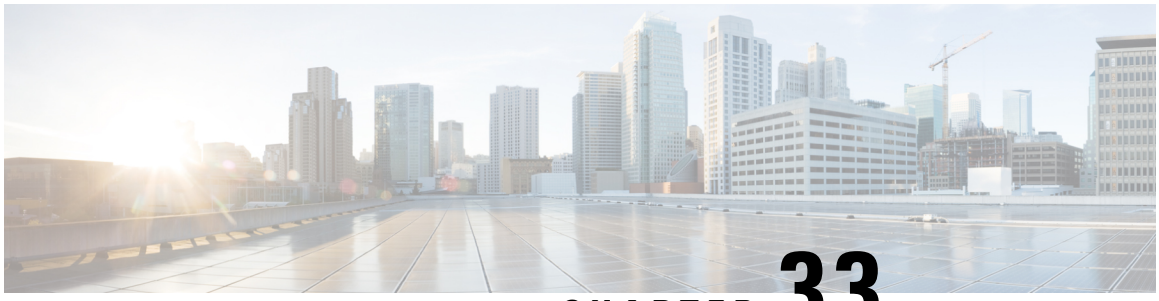
Command Changes

Use the following CLI configuration to limit the Secondary RAT Usage in CDR.

```
configure
   context context_name
   gtpp group group_name
      [no] limit-secondary-rat-usage
      end
```

NOTES:

- **limit-secondary-rat-usage**: Enables limiting the number of Secondary RAT Usage reports in CDR.
- **no**: Disables limiting the number of Secondary RAT Usage reports in CDR.



CHAPTER 33

Support to Add Two Additional Attributes in EDR

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	Enabled - Always-on
Related Documentation	*MME Administration Guide*

Revision History

Revision Details	Release
First Introduced	21.23

Support to Add Two Additional Attributes in EDR

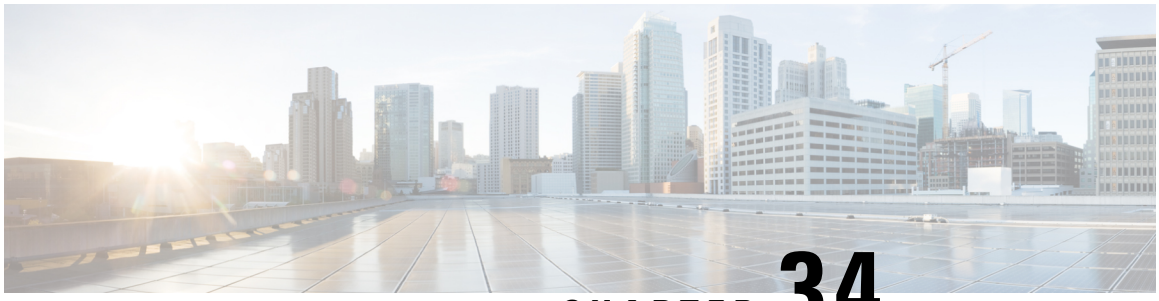
In the existing Event Data Record (EDR) fields, there are a total of 27 fields and currently, 2 more fields are added to the event-data-record and they are mme-ue-s1ap-id and procedure-start-time.

The event report includes the information in CSV format as shown in the table given below:

Support to Add Two Additional Attributes in EDR

Table 30: Information Fields in the EDR

SI.No	Description	Format Information	Range
28	mme-ue-s1ap-id	Number	0 to 4294967295
29	procedure-start-time	YYYY-MM-DD+HH:MM:SS	



CHAPTER 34

Suppressing Handover Request for VoWiFi IR Subscribers

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* • *AAA Interface Administration and Reference* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
The PGW selection mechanisms in ePDG is enhanced to provide suppressing handover request for VoWiFi International Roaming (IR) subscribers.	21.23

Feature Description

The selection mechanism is enhanced, so that whenever the IR subscribers do a VoLTE to VoWiFi handover (HO) call, the ePDG selects the dedicated locally configured P-GW for the IR in the ePDG-service and forwards it. Once the HO is successfully completed, the termination of UE context in LTE is not supported on ePDG and the requests received in this dedicated ePDG is expected to be always IR HO.

How it Works

Use the following command to enable IR feature under the ePDG service is:

handover international-roamer suppress

Use the following command to disable this feature under the ePDG service:

no handover international-roamer suppress

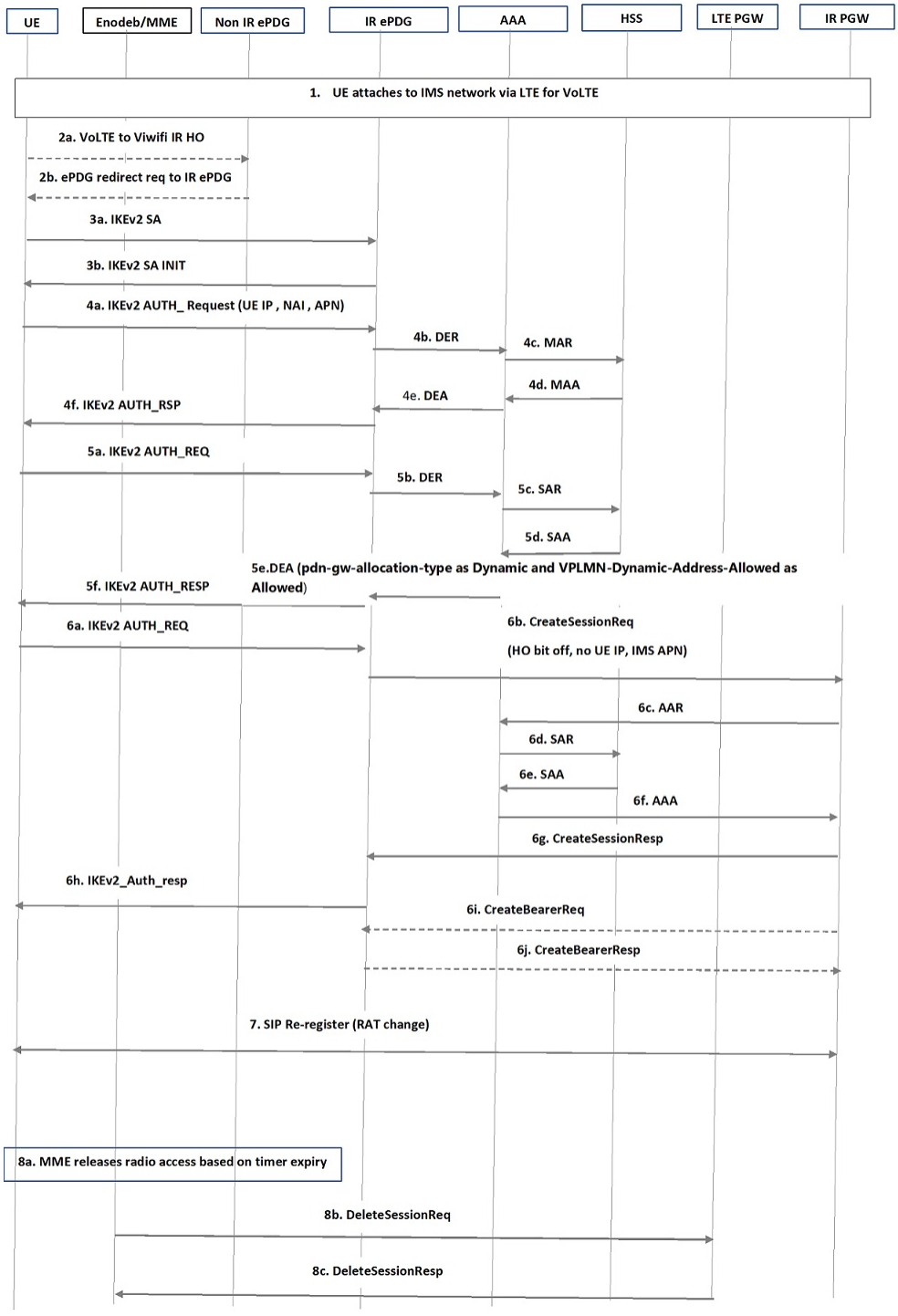
Note This CLI is disabled by default.

Enabling the CLI in normal ePDG impacts the normal ePDG HO call flows. The following warning message is displayed on enabling the feature:

VoLTE to VoWi-Fi IR HO Call Flows

The following call flow diagram describes the VoLTE to VoWi-Fi IR HO to IR ePDG.

Figure 8: VoLTE to VoWi-Fi IR HO to IR ePDG



Step	Description
1	The International Roamer (IR) UE attaches to LTE for availing IMS network (IMS APN).
2	• If the UE does handover (HO) to a Wi-Fi network, ensure that the UEAP sends the request to IR supported ePDG, and not to the Non-IR supported ePDG. • If the UE sends the request to a non-IR supported ePDG, the ePDG sends redirect request indication to the UE with the correct information. UE sends HO requests to the IR ePDG only if UE redirection is supported. This feature does not support redirection and it must be handled outside the ePDG.
3	UE sends IKv2_SA_INIT to IR ePDG and receives a response from ePDG to establish the tunnel.
4	• The UE sends the user identity (in the IDi payload) and the APN information (in the IDr payload, IMS APN in case) in this first message of the IKE_AUTH phase, and begins negotiation of child security associations. When the MAC ULI feature is enabled, the root NAI used has the following format: "0<IMSI>AP_MAC_ADDR:nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org" **Note** The UE omits the AUTH parameter to indicate to the ePDG that it wants to use EAP over IKEv2. The user identity complies with the NAI format specified in TS 23.003 containing the IMSI, as defined for EAP-AKA in RFC 4187. The UE IP address is suppressed while sending CSReq message to P-GW. • The UI and APN are forwarded to the AAA server. The AAA server verifies the subscriber profile fetched from HSS and the 3GPP AAA server initiates the authentication challenge. Id the user identity is not requested again then ePDG responds to IKA_INIT.
5	UE sends the Authentication challenge-response and verifies with AAA, then responds to UE for authentication completion. During the DEA (Diameter EAP Answer) reply from AAA in this process, the AAA sets "VPLMN-Dynamic-Address-Allowed" as allowed and "PDN-GW-Allocation-Type" as dynamic.
6	Based on the P-GW identified in Step 5, the ePDG sends the CreateSessionReq with IMS APN, Handoff bit set to “off” to P-GW so that P-GW will consider this as a fresh attach. Since the new P-GW is different from the LTE P-GW, the UE context will not be present and it will allocate a new IP, which is forwarded to UE through ePDG. The new P-GW updates the UE and APN information to AAA and then to HSS. Optionally based on the number of dedicated bearers, the Create Bearer procedure will happen.
7	Since the RAT has changed from LTE to Wi-Fi, the SIP re-register will happen.
8	P-GW will not trigger the DeleteSessionReq for LTE bearers, as UE gets attached to a different P-GW after Wi-Fi handover. On the timer expiry (probably periodic TAU timer) expiry, the MME releases the LTE bearers.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show epdg-service statistics suppress-ir-handover

The output of this command includes the following fields:

Fields/Counters	Description
Attempts: 1	Total number of ePDG sessions for which international roaming handoff attempted on international roaming HO suppression supported ePDG.
Success: 1	Total number of ePDG sessions for which international roaming handoff attempts succeeded on international roaming HO suppression supported ePDG.
Failures: 0	Total number of ePDG sessions for which international roaming handoff attempts failed on international roaming HO suppression supported ePDG.

show epdg-service name *name*

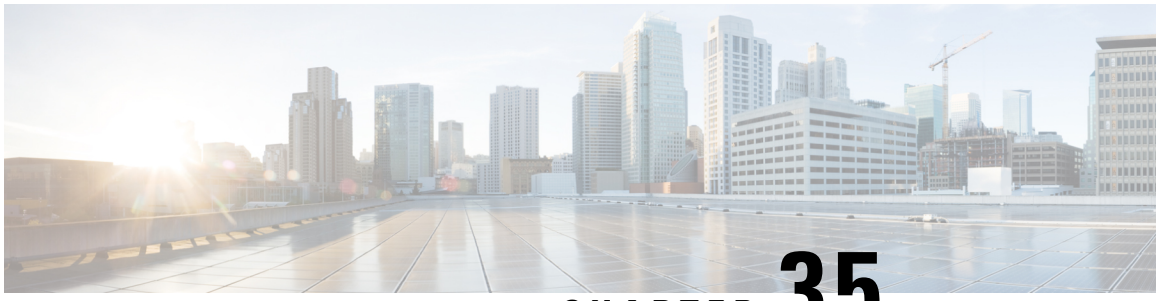
The output of this command includes the following fields to check whether IR suppress handover is enabled or disabled.

Fields/Counters	Description
Suppress International Roamer Handover	Specifies if the suppress international roamer HO is enabled or disabled.

Bulk Statistics

The ePDG schema supports the following bulk statistics for suppressing handover request for VoWiFi IR subscribers:

Bulk Statistics	Description
suppress-intr-roaming-ho-attempts	Indicates the total number of ePDG sessions for which international roaming handoff attempted. This increments when international roaming handoff is attempted on international roaming HO suppression supported ePDG.
suppress-intr-roaming-ho-success	Indicates the total number of ePDG sessions for which international roaming handoff attempts succeeded. This increments when international roaming handoff attempt succeeds on international roaming HO suppression supported ePDG.
suppress-intr-roaming-ho-failures	Indicates the total number of ePDG sessions for which international roaming handoff attempts failed. This increments when international roaming handoff attempt fails on international roaming HO suppression supported ePDG.



CHAPTER 35

Timeout Exclusion from CSFB Counters

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	Enabled- Always-on
Related Changes in This Release	Not applicable
Related Documentation	• *MME Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First Introduced	21.23

Feature Description

Degradation occurs in the network statistics when there is specific Mobile Terminated (MT) Circuit Switch Fallback (CSFB) paging request timeout error occur. When the UE (User Equipment) is in idle mode, the MME to eNB CSFB based paging requests are ignored by the eNB. This results in MME recording the specific MT CSFB paging request timeout error and thus paging re-transmission timeout error gets incremented in the relevant MT CSFB failure bulkstat counters.

To ignore the paging re-transmission timeout error being incremented in the relevant MT CSFB failure bulkstat counters, the following new configuration commands are implemented under mme-service:

1. count csfb-mt-voice-paging timeouts
2. count csfb-mt-sms-paging timeouts

These new commands instruct the MME to ignore the recording of this specific MT CSFB paging request timeout error in the bulkstat counters “csfb-nw-voice-failures” and “csfb-nw-sms-failures” respectively.

Enabling and Disabling Voice and SMS for Paging Re-transmission Timeout

Use the following configuration commands to enable and disable voice and SMS for paging re-transmission timeout:

```
config
   context context_name
      mme-service service_name
          [ no ]count csfb-mt-voice-paging timeouts
          [ no ]count csfb-mt-sms-paging timeouts
     end
```

NOTES:

- **count csfb-mt-voice-paging timeouts**: Configures specific MT CSFB Voice paging request timeout error.
- **count csfb-mt-sms-paging timeouts**: Configures specific MT CSFB SMS paging request timeout error.

Show Command and Output

show mme-service all|name

The output of this command displays the two new parameters under mme-service and there status are as follows:

- csfb-nw-voice-pagingt imeouts: Enabled/Disabled
- csfb-nw-sms-paging timeouts: Enabled/Disabled

The current bulkstat counters “csfb-nw-voice-failures” and “csfb-nw-sms-failures” can be verified either through the bulkstats feature or the “show mme-service statistics” command as normal.