Release Change Reference, StarOS Release 21.26

First Published: 2021-12-22

Last Modified: 2023-04-04

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

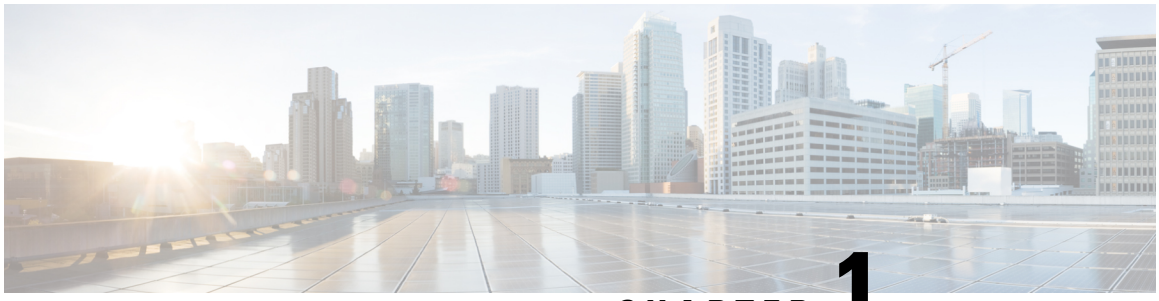
Conventions Used

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**



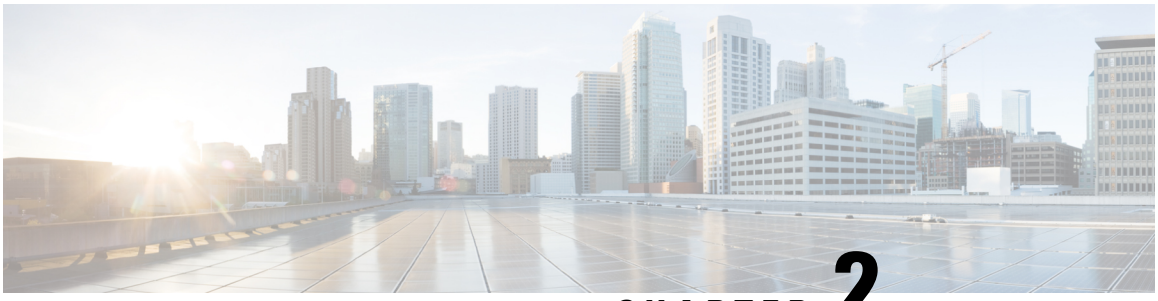
CHAPTER 1

Release 21.26 Features and Changes Quick Reference

Release 21.26 Features and Changes

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
Bias-free Terminologies, on page 11	All	21.26
Bulk Statistics for Average Data Rate Per IP Pool, on page 15	• GGSN • P-GW	21.26
Custom26 Dictionary for Gy 5G NSA	• P-GW • SAEGW • S-GW	21.26
Customizing Access-Link IP Fragmentation	• GGSN • P-GW • SAEGW	21.26
Customizing Last User Location Information	• P-GW • SAEGW	21.26
Customizing TAC Field in CDR	• P-GW • SAEGW	21.26
DSR Flag and PTW Subscription Withdrawal on eDRX, on page 37	• C-SGN • MME	21.26

Features / Behavior Changes	Applicable Product(s) / Functional Area	Release Introduced / Modified
ePDG Interworking with SMF+P-GW-IWK Support, on page 47	ePDG	21.26
Handling CC-Request-Number AVP during Assume Positive State, on page 71	P-GW	21.26.h5 21.26.19
No IMSI or MSISDN Included in LRR for VoLTE EM Call from User of Foreign Network, on page 73	MME	21.26
IPv4 and IPv6 Address Alignment, on page 75	ePDG	21.26
Monitoring Offloading and Onloading VPP Flow Transactions, on page 77	P-GW	21.26
Multiple Customized PCO Support, on page 81	• GGSN • P-GW	21.26
Password Expiration Notification, on page 87	P-GW	21.26
Password Change Option in Warning Period, on page 91	• ASR 5500 • VPC-DI • VPC-SI	21.26.h5 21.26.15
Secondary RAT Usage Report in CDR Records, on page 93	• P-GW • SAEGW • S-GW	21.26
Sponsored Data AVPs on Gx Interface to PCRF	• P-GW • SAEGW	21.26
Support for 187 and 188 Information Element Types on S2b Interface, on page 105	ePDG	21.26.17
Support for 187 and 188 Information Element Types on S5 and S8 Interfaces, on page 109	MME	21.26.17
VPP Flow Statistics, on page 113	• P-GW • SAEGW	21.26



CHAPTER 2

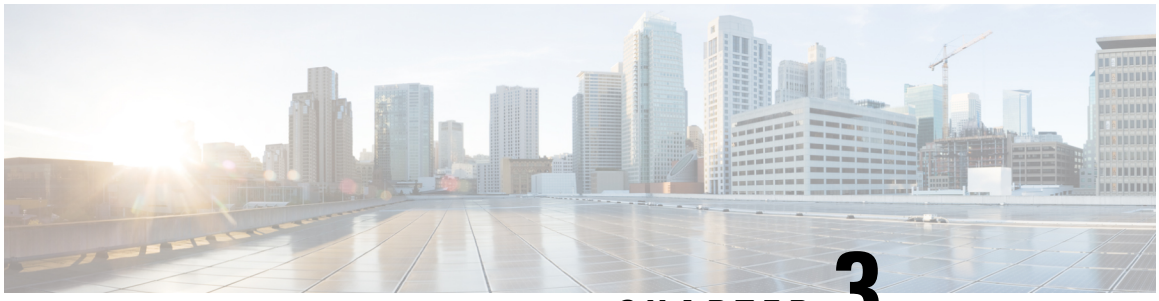
Feature Defaults Quick Reference

Feature Defaults

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

Feature	Default
Bias-free Terminologies	Enabled - Always-on
Bulk Statistics for Average Data Rate Per IP Pool	Enabled - Always-on
Custom26 Dictionary for Gy 5G NSA	Disabled - Configuration Required
Customizing Access-Link IP Fragmentation	Enabled - Always-on
Customizing Last User Location Information	Disabled - Configuration Required
Customizing TAC Field in CDR	Disabled - Configuration Required
DSR Flag and PTW Subscription Withdrawal on eDRX	Disabled - Configuration Required
ePDG and SMF+P-GW Interworking	Disabled – Configuration Required
Handling CC-Request-Number AVP during Assume Positive State	Disabled - Configuration Required
IMSI not Included in LRR	Disabled – Configuration Required
IPv4 and IPv6 Address Alignment	Disabled – Configuration Required
Monitoring Offloading and Onloading VPP Flow Transactions	Enabled - Configuration Required
Multiple Customized PCO Support	Disabled – Configuration Required
Password Expiration Notification	Enabled - Always-on
Password Change Option in Warning Period	Enabled - Always-on
Secondary RAT Usage Report in CDR Records	Disabled - Configuration Required

Feature	Default
Sponsored Data AVPs on Gx Interface to PCRF	Disabled - Configuration Required
Support for 187 and 188 Information Element Types on S2b Interface	Disabled - Configuration Required
Support for 187 and 188 Information Element Types on S5 and S8 Interfaces	Disabled - Configuration Required
VPP Flow Statistics	Disabled - Configuration Required



CHAPTER 3

Bulk Statistics Changes Quick Reference

This chapter identifies bulk statistics changes added to, modified for, or deprecated from the StarOS 21.26 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 21.26 include:

New Bulk Statistics

epdg-interworking-5g schema

The following bulk statistics are added in the epdg-interworking-5g schema as part of the ePDG and SMF+P-GW Interworking feature:

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

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

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

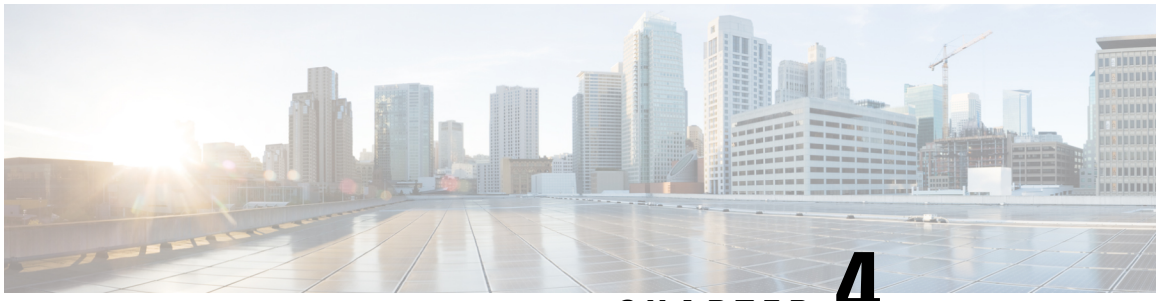
Bulk Statistics Variables	Description
iwk5g-local-pgw-fallback-failed	The number of times that a session fails to connect to P-GW is selected through the fallback algorithm.
iwk5g-local-pgw-fallback-noalt-pgw	The number failed attempts to all P-GW, and there is no alternate P-GW available to attempt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

Modified Bulk Statistics

None in this release.

Deprecated Bulk Statistics

None in this release.



CHAPTER 4

SNMP MIB Changes in StarOS 21.26

This chapter identifies SNMP MIB objects, alarms and conformance statements added to, modified for, or deprecated from the StarOS 21.26 software release.

SNMP MIB Alarm Changes for 21.26

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

SNMP MIB Conformance Changes for 21.26

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

SNMP MIB Object Changes for 21.26

This section provides information on SNMP MIB alarm changes in release 21.26.

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

New SNMP MIB Object

There are no new SNMP MIB objects in this release.

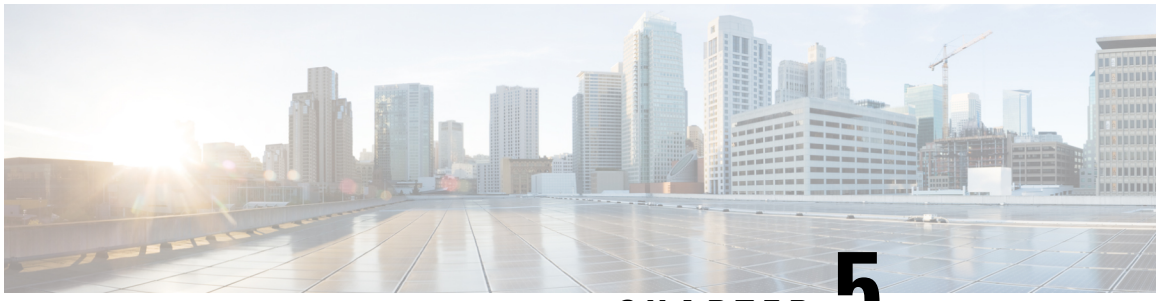
Modified SNMP MIB Object

This section identifies new SNMP MIB alarms available in release 21.26.

- starSRPConfigInSync
- starNicBondChange

Deprecated SNMP MIB Object

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



CHAPTER 5

Bias-free Terminologies

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	All
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled – Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

Our product and documentation set 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.

With this release, biased terms present in CLI commands and logs are being replaced with bias-free terms.

Note Biased CLI configuration is also supported in this release. However, in the show CLI commands you will not be able to see Biased terms in the output.

The following table provides the list of CLI commands that have been updated to replace the biased terms.

CLI Commands in Releases Prior to 21.26	CLI Commands in 21.26 and Later Releases
clear blacklisted-gtpu-bind-address	**clear blockedlisted-gtpu-bind-address**
clear mme-service sgw-blacklist	**clear mme-service sgw-blockedlist**
clear mme-service sgw-blacklist sgw-ip	**clear mme-service sgw-blockedlist sgw-ip**
clear mme-service sgw-blacklist mme-service-name	**clear mme-service sgw-blockedlist mme-service-name**
clear user-plane-service url-blacklisting	**clear user-plane-service url-blockedlisting**.
clear user-plane-service url-blacklisting statistics	**clear user-plane-service url-blockedlisting statistics**.
crypto blacklist file	**crypto blockedlist file**
crypto blacklist file update	**crypto blockedlist file update**
crypto whitelist	**crypto permitlist**
default url-blacklisting	**default url-blockedlisting**
default url-blacklisting action	**default url-blockedlisting action**
diameter msg-type ccrt suppress-blacklist-reporting	**diameter msg-type ccrt suppress-blockedlist-reporting**
diameter reauth-blockedlisted-content	**diameter reauth-blockedlisted-content**
flow end-condition timeout url-blacklisting	**flow end-condition timeout url-blockedlisting**
link-aggregation master group	**link-aggregation primary group**
require diameter-proxy master-slave	**require diameter-proxy primary-secondary**
sgw-blacklist	**sgw-blockedlist**
sgw-blacklist timeout	**sgw-blockedlist timeout**
sgw-blacklist timeout 8 msg-timeouts-per-min	**sgw-blockedlist timeout 8 msg-timeouts-per-min**
show active-charging url-blacklisting	**show active-charging url-blockedlisting**
show crypto blacklist	**show crypto blockedlist**
show crypto whitelist	**show crypto permitlist**

CLI Commands in Releases Prior to 21.26	CLI Commands in 21.26 and Later Releases
show crypto whitelist file	**show crypto permitlist file**
show mme-service sgw-blacklist	**show mme-service sgw-blockedlist**
show user-plane-service inline-services url-blacklisting statistics	**show user-plane-service inline-services url-blockedlisting statistics**
snmp trap suppress BlackListingDBFail	**snmp trap suppress BlockedListingDBFail**
snmp trap suppress BlacklistingDBFailClear	**snmp trap suppress BlockedlistingDBFailClear**
snmp trap suppress BlackListingDBUpgradeFail	**snmp trap suppress BlockedListingDBUpgradeFail**
snmp trap suppress BlacklistingDBUpgradeFailClear	**snmp trap suppress BlockedlistingDBUpgradeFailClear**
url-blacklisting	**url-blockedlisting**
url-blacklisting action	**url-blockedlisting action**
url-blacklisting action discard content-id	**url-blockedlisting action discard content-id**
url-blacklisting match-method	**url-blockedlisting match-method**
whitelist	**permitlist**

The help string of the following CLI commands has been updated to replace the biased terms:

- **act-mmgr-inst**
- **diameter enable-quota-retry**
- **diameter enable-quota-retry end-user-service-denied**
- **ispc link A**
- **sgsn op enable ccpu debug_log facility mmgr**
- **sgsn retry-unavailable-ggsn**
- **sgsn test mmgr**
- **show ssi ccpu debug_log facility**
- **system packet-dump di-net card 3 bond a/b**
- **uidh-insertion server-name svc bypass wl-lookup**

Downgrade Procedure

When you downgrade from 21.26.0 to any prior release version (21.x.y), the biased term keywords used in CLI commands get lost due to the biased language changes. To have smooth backward compatibility transition along with bias-free terms in CLI commands, follow the prerequisite before downgrading to the lower versions:

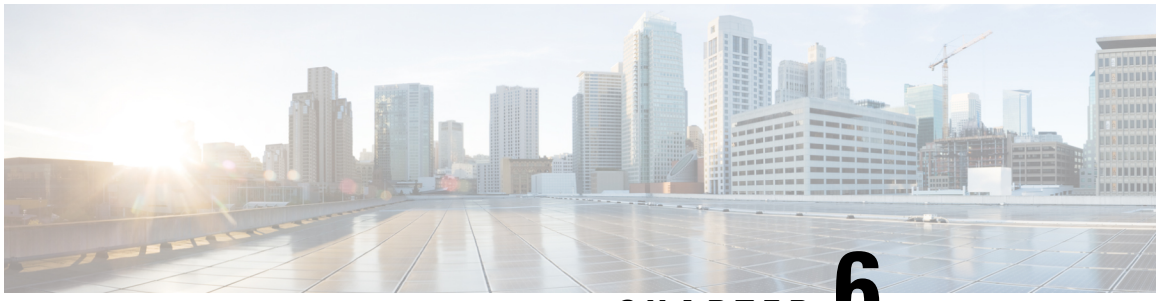
Prerequisite:

- Before upgrade from a lower version to 21.26.0, backup the existing configurations.

Downgrade the chassis with the version 21.x.y using the backed up configuration.

Note After the downgrade, the show configuration will not have the biased terms CLI.

If you fail to save the configurations before upgrade, configure the required biased CLI commands manually, save, and reload the chassis.



CHAPTER 6

Bulk Statistics for Average Data Rate Per IP Pool

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The number of IP pool groups is increased from 2000 to 5000.	21.26
First introduced.	21.3

Feature Description

The bulk statistics support is enhanced to fetch the subscriber average data rate per IP pool (cumulative of all session managers). The average data rate consists of all the IP pools configured in the system.

The bulk statistics collection time is enhanced for the datarate-ippool schema. This schema supports up to 5000 IP pool groups when configured.

Monitoring and Troubleshooting

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

Bulk Statistics

This feature supports the following bulk statistics:

Datarate-IPPool Schema

The following bulk statistics are added to the Datarate-IPPool schema:

- sess-datarate-ippool-name—Indicates the name of the IP pool for which average data rates are fetched.
- sess-ave-rate-fuser-bps—Indicates the average data-rate (bits/sec) from the user in uplink direction per IP pool basis.
- sess-ave-rate-tuser-bps—Indicates the average data-rate (bits/sec) to the user in downlink direction per IP pool basis.
- sess-ave-rate-fuser-pps—Indicates the average packets/second from the user in uplink direction per IP pool basis.
- sess-ave-rate-tuser-pps—Indicates the average packets/second to the user in downlink direction per IP pool basis.

Show Commands and/or Outputs

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

show bulkstats schema

Table 1: show bulkstats schema Command Output Descriptions

Field	Description
Bulk Statistics Server Configuration:	
Server State	Indicates the server state—enabled or disabled.
File Limit	Indicates the file size limit in KB.

Field	Description
Sample Interval	Indicates the sampling interval.
Transfer Interval	Indicates the transfer interval.
Receiver Mode	Indicates the receiver mode.
Local File Storage	Indicates the local file storage.
Bulk Statistics Server Statistics:	
Records awaiting transmission	Indicates the number of records awaiting transmission.
Bytes awaiting transmission	Indicates the number of bytes awaiting transmission.
Total records collected	Indicates the total number of records collected.
Total bytes collected	Indicates the total number of bytes collected.
Total records transmitted	Indicates the total number of records transmitted.
Total bytes transmitted	Indicates the total number of bytes transmitted.
Total records discarded	Indicates the total number of records discarded.
Total bytes discarded	Indicates the total number of bytes discarded.
Last collection time required	Indicates the last collection time required.
Last transfer time required	Indicates the last transfer time required.
Fine n	
Remote File Format	The remote file format—for example, %date%-%time%
File Header	The file's header.
File Footer	The file's footer.
File Statistics:	
Records awaiting transmission	Indicates the number of records awaiting transmission.
Bytes awaiting transmission	Indicates the number of bytes awaiting transmissions.
Total records collected	Indicates the total number of records collected.
Total bytes collected	Indicates the total number of bytes collected.
Total records transmitted	Indicates the total number of records transmitted.
Total bytes transmitted	Indicates the total number of bytes transmitted.
Total records discarded	Indicates the total number of records discarded.
Total bytes discarded	Indicates the total number of bytes discarded.

Field	Description
Last transfer time required	Indicates the last transfer time required.
No successful data transfers	Indicates the total number of successful data transfers.
No attempted data transfers	Indicates the total number of attempted data transfers.

show bulkstats data

Table 2: show bulkstats data Command Output Descriptions

Field	Description
Bulk Statistics Server Configuration:	
Server State	Indicates the server state—enabled or disabled.
File Limit	Indicates the file size limit in KB.
Sample Interval	Indicates the sampling interval.
Transfer Interval	Indicates the transfer interval.
Receiver Mode	Indicates the receiver mode.
Local File Storage	Indicates the local file storage.
Historical Data Collection	Indicates the Historical Data Collection state—enabled or disabled.
Bulk Statistics Server Statistics:	
Records awaiting transmission	Indicates the number of records awaiting transmission.
Bytes awaiting transmission	Indicates the number of bytes awaiting transmission.
Total records collected	Indicates the total number of records collected.
Total bytes collected	Indicates the total number of bytes collected.
Total records transmitted	Indicates the total number of records transmitted.
Total bytes transmitted	Indicates the total number of bytes transmitted.
Total records discarded	Indicates the total number of records discarded.
Total bytes discarded	Indicates the total number of bytes discarded.
Last collection time required	Indicates the last collection time required.
Last transfer time required	Indicates the last transfer time required.
No successful data transfers	Indicates the total number of successful data transfers.
No attempted data transfers	Indicates the total number of attempted data transfers.

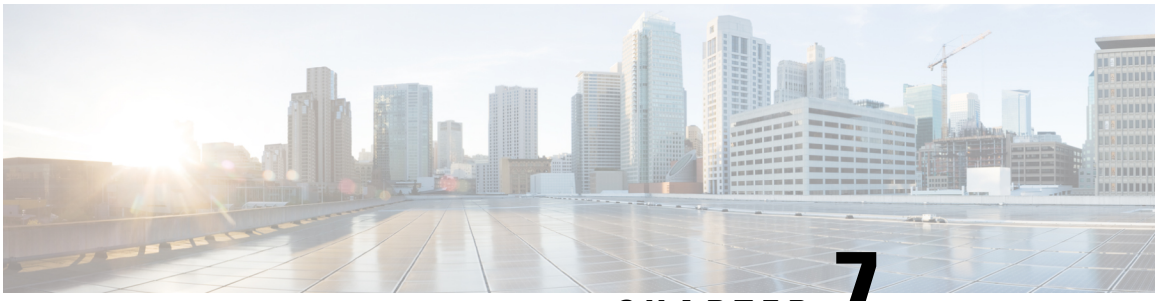
Field	Description
Fine n	
Remote File Format	The remote file format—for example, %date%-%time%
File Header	The file's header.
File Footer	The file's footer.
No bulkstats receivers	Indicates the total number of bulk statistics collection servers configured.
File Statistics:	
Records awaiting transmission	Indicates the number of records awaiting transmission.
Bytes awaiting transmission	Indicates the number of bytes awaiting transmission.
Total records collected	Indicates the total number of records collected.
Total bytes collected	Indicates the total number of bytes collected.
Total records transmitted	Indicates the total number of records transmitted.
Total bytes transmitted	Indicates the total number of bytes transmitted.
Total records discarded	Indicates the total number of records discarded.
Total bytes discarded	Indicates the total number of bytes discarded.
Last transfer time required	Indicates the last transfer time required.
No successful data transfers	Indicates the total number of successful data transfers.
No attempted data transfers	Indicates the total number of attempted data transfers.
Handoff Statistics	
epdg-handoff-disc	Configures LTE to Wi-Fi HO disconnect reason statistics.
show epdg-service statistics handoff-disc-reasons	Displays the statistics corresponding to LTE to Wi-Fi HO disconnect reasons for all services.
clear epdg-service statistics handoff-disc-reasons	Removes the statistics corresponding to LTE to Wi-Fi HO disconnect reasons for all services.

show subscribers data-rate ip-pool <pool_name>

Table 3: show subscribers data-rate ip-pool <pool_name> Command Output Descriptions

Field	Description
pk rate from user (bps)	The peak data rate, in bits per second, obtained for data sent from the subscriber to the network during the last sampling period.

Field	Description
peak rate to user (bps)	The peak data rate, in bits per second, obtained for data received from the network by the subscriber during the last sampling period.
ave rate from user (bps)	The average data rate, in bits per second, obtained for data sent from the subscriber to the network during the last sampling period.
ave rate to user (bps)	The average data rate, in bits per second, obtained for data received from the network by the subscriber during the last sampling period.
sust rate from user (pps)	The mean data rate, in packets per second, obtained for data sent from the subscriber to the network during the last three sampling periods.
sust rate to user(pps)	The mean data rate, in packets per second, obtained for data received from the network by the subscriber during the last three sampling periods.



CHAPTER 7

Custom26 Dictionary for Gy 5G NSA

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-GW • S-GW • SAEGW
Applicable Platform(s)	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *5G Non Standalone Solution Guide* • *AAA Interface Administration and Reference* • *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

Revision History

The 5G NSA solution for SAEGW supports dcca-custom26 dictionary.	21.26
The 5G NSA solution for SAEGW supports Secondary RAT Usage IE during GnGp handover.	21.22
The 5G NSA solution for SAEGW supports dcca-custom1, dcca-custom7 and dcca-custom8 dictionaries.	21.11
The 5G NSA solution for SAEGW supports the following functionality: • P-GW Custom Dictionaries support over Gz for extended bitrate • S-GW Custom Dictionaries support over Gz for extended bitrate • P-GW Custom Dictionaries support over Gy and Rf for extended bitrate • S-GW support of Secondary RAT Data Usage Report in Gz CDRs	21.10
The 5G NSA solution for SAEGW supports the following functionality: • P-GW support of Secondary RAT Data Usage Report in Gz CDRs • P-GW support of Secondary RAT Data Usage Report in Rf CDRs • S-GW and P-GW support of statistics for DCNR PDNs	21.9
The 5G NSA solution is qualified on the ASR 5000 platform.	21.5
The 5G NSA solution for SAEGW supports the following functionality: • Feature License • Dedicated Bearers • Gy interface • URLLC QCI	21.8
First introduced.	21.6

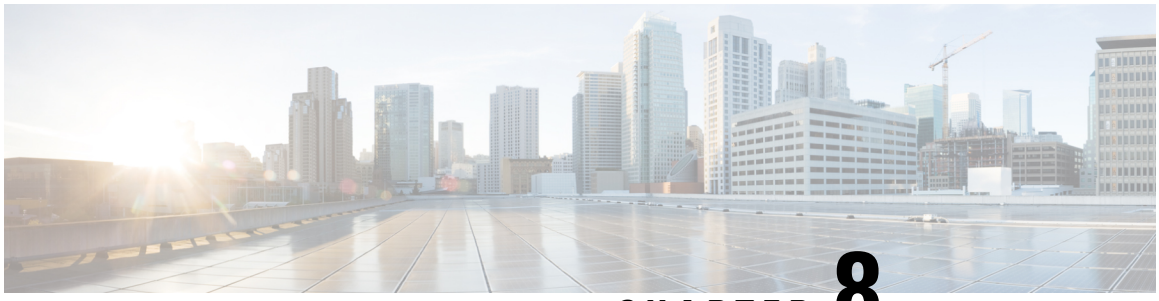
Feature Description

Whenever P-GW and SAEGW receives GBR and APN-AMBR values greater than 4.2Gbps, P-GW and SAEGW provides support for the following extended bit rate AVPs in custom26 dictionary over Gy Diameter interface:

- Extended-Max-Request-BW-UL
- Extended-Max-Requested-BW-DL
- Extended-GBR-UL
- Extended-GBR-DL

- Extended-APN-AMBR-UL
- Extended-APN-AMBR-DL

For more information, see the *5G NSA for SAEGW* chapter in the *5G Non-standalone Solution Guide*.



CHAPTER 8

Customizing Access-Link IP Fragmentation

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Description

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

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

Configuring Access-Link IP Fragmentation

Configuring access-link IP fragmentation involves the following steps:

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

Configuring Global Level Access-Link IP Fragmentation

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

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

NOTES:

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

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

Configuring APN Level Access-Link IP Fragmentation

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

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

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

NOTES:

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

Configuring Access-Link Fastpath to Enforce APN MTU

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

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

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

NOTES:

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

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

Monitoring and Troubleshooting

This section provides information regarding show commands and their outputs.

Show Commands and Output

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

show configuration access-link

The output of this command displays the following field.

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

show configuration access-link verbose

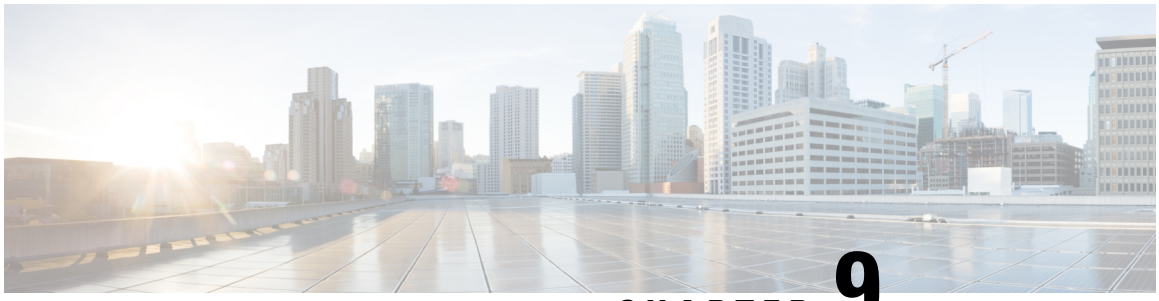
The output of this command displays the following field.

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

show config apn <apn_name>

The output of this command displays the following field.

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



CHAPTER 9

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.

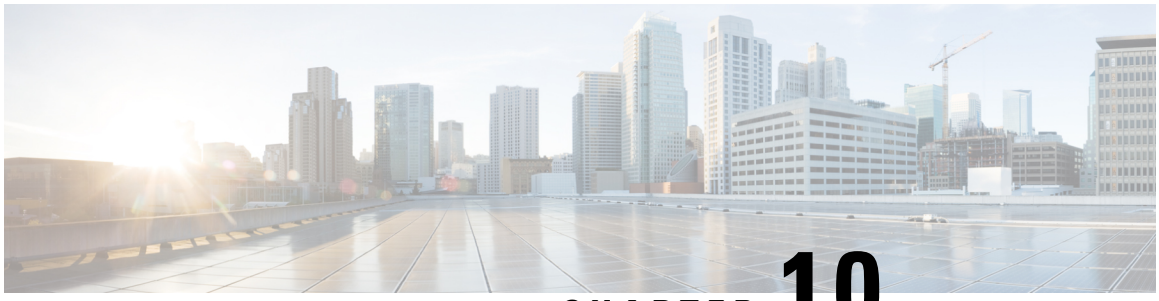
Show Commands and Output

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 10

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.

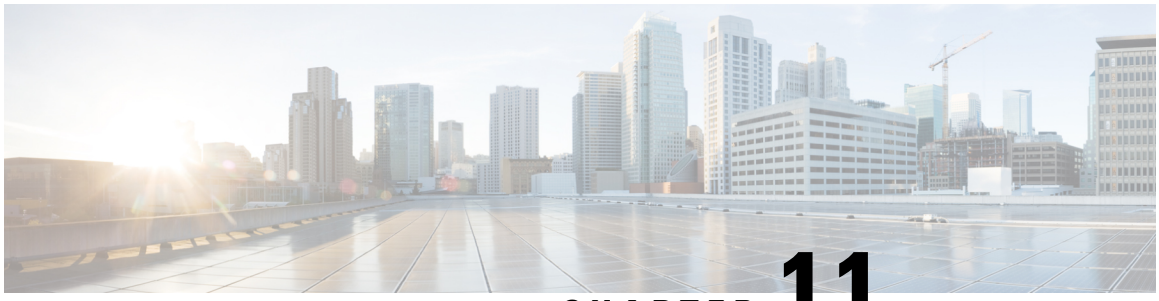
Show Commands and Output

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 11

DSR Flag and PTW Subscription Withdrawal on eDRX

Feature Summary and Revision History

Summary Data

Applicable Products or Functional Area	• C-SGN • MME
Applicable Platforms	• ASR 5500 • UGP • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required (eDRX feature) Enabled - Configuration Required (eDRX GPS time support in 21.4)
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *Statistics and Counters Reference* • *Ultra IoT C-SGN Administration Guide* • *MME Administration Guide*

Revision History

Revision Details	Release
Support is added for Delete Subscriber Data Request (DSR) flag bits 28 and 30 Paging Time Window (PTW) subscription withdrawal with eDRX.	21.26
Paging eDRX H-SFN changed to 10 bits counter.	21.11.3
The eDRX feature is enhanced to support H-SFN Start time configuration in GPS format and H-SFN Reference time in GPS and UTC format. The **edrx** command in the MME Service Configuration mode is enhanced in this release. For more information, see *Configuring Hyper SFN Synchronization* chapter in the *MME Administration Guide*. The feature default for this enhancement is "Enabled - Configuration Required".	21.4
The feature is tested and qualified on the ASR 5500 platform.	21.3
The enhancements in the N5.1 release include: • MME supports configuration of the T3415 paging timeout value. MME uses the T3415 timer for eDRX UEs. • The **edrx** CLI command is enhanced to support DL Buffering Suggested Packet Count in DDN ACK when unable to page UE. • Support of the DL-Buffering-Suggested-Packet-Count AVP	N5.1 (21.1.V0)
First introduced.	21.0

Feature Description

The MME is enhanced to support Delete Subscriber Data Request (DSR) flags bits 28 and 30, and Paging Time Window (PTW) subscription withdrawal with eDRX. This feature supports the eDRX related Radio Access Technology (RAT) AVP in the DSDR message. This feature is beneficial to the Session Manager (SessMgr) running the MME application stack.

For more information, see the *eDRX Support on the MME* chapter in the *MME Administration Guide*.

How It Works

In MME, Home Subscriber Server (HSS) sends eDRX and PTW information as part of Update Location Answer (ULA) and/or Delete Subscriber Data Request (DSDR). After ULA, when MME receives a DSDR message with 28th and 30th bit set, MME deletes the stored HSS subscription data related to eDRX accordingly. The 28th bit set is for PTW withdrawal and 30th bit set is for eDRX withdrawal.

If MME receives the eDRX-Related-RAT AVP (1705) with the DSR flag set for eDRX withdrawal, the MME compares the RAT type of the subscriber session with the received RAT type in eDRX-Related-RAT AVP. If it matches, then the MME resets the eDRX information to the values negotiated in the Attach Request.

Monitoring and Troubleshooting

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

Show Commands and Outputs

This section provides information about the show commands and outputs to displays the current Paging eDRX information of a subscriber.

show mme-service session full all | grep Paging

Table 4: show mme-service session full all | grep Paging Command Output Descriptions

Field	Description
SessMgr Instance	The Session Manager instance managing this session.
Paging eDRX	The following are the paging eDRX parameters: • eDRX cycle length • PTW
MSID	The UE identity (MS Identity) of a connected subscriber to an MME service, and whether the subscriber is unauthenticated (such as during emergency attach).
Callid	The call identity in 8 digit hex number of connected calls to an MME service.
MME Service	The name of the serving MME service of which information is displayed.
MME HSS Service	The name of the serving MME-HSS service which is used for AAA for this subscriber with HSS on S6a interface.
EGTP S11 Service	The name of the serving eGTP service which is used for connectivity between MME and S-GW on S11 interface.
MME S1 Address	The IP address of MME used for connecting with eNodeB on S1-MME interface.
EGTP S11 Address	The IP address assigned to eGTP service which is used for connectivity between MME and S-GW on S11 interface.
ME Identity	The mobile equipment identity of connected UE.
GUTI	The Globally Unique Temporary Identifier (GUTI) used for this subscriber session. GUTI is constructed with following identifiers: • PLMN (MMC and MNC) • MME Group ID (MMEGI) • MME Code (MMEC) • MME TMSI (M-TMSI)

Field	Description
MSISDN	The Mobile Station International ISDN Number (MSISDN) of connected EPS subscriber to an MME service.
EMM State	The status of EPS Mobility Management (EMM) session of connected subscriber. Possible status are: • Registered • Connected
ECM State	The status of EPS Connection Management (ECM) session of connected subscriber. Possible status are: • Registered • Connected • Idle
Attach type	Indicates the type of UE attachment of active subscriber to MME service, for example: Emergency or Initial EPS.
Active SGW S11 Addr	The IP address of S-GW connected to MME on S11 interface.
SGW Control TEID	Displays the TEID of the S-GW currently serving the UE.
UE Offloading	Displays the UE offload state for load rebalancing. Possible values are None, Marked, In-Progress and Done.
UE Reachability Timer	The configured value of the mobile reachability timer set for tracking UE in EMM session.
Remaining Time	The remaining time in seconds out of the configured value of the mobile reachability timer in the EMM session.
Paging Proceed Flag (PPF)	The current state of the Paging Proceed Flag indicating whether or not the UE is sending periodic TAUs within the span of the mobile reachability timer. If the UE fails to send a TAU within the timer value, this flag is set to "Paging Disabled" indicating that the MME is no longer paging the UE.
ISR Status	Displays if the session is using Idle mode Signaling Reduction (ISR). Possible configurations are Activated or Not activated.
Low Access Priority Indication	Displays whether this session has LAPI indicator in any of attach/extended service/TAU/bearer resource allocation/bearer resource modification/PDN connectivity requests.
Initial UE establishment cause	Displays the establishment cause as set in the Initial UE message: Delay Tolerant Access / High Priority Access / Emergency / MT-Access / Unknown
Peer SGSN	Displays the IP address of the SGSN which has a context for this UE in support of Idle mode Signaling Reduction (ISR). A Peer SGSN address is only shown when ISR is activated for this session.

Field	Description
UE Capability Information	This group shows the UE Capability information for connected UE received by an MME service.
Radio Capability	The radio capability information received by an MME service for connected UE in UE capability exchange message.
Radio Capability for Paging	The radio capability information received by an MME service for paging the UE. This field displays the value in hexadecimal format if the UE receives "UE Radio Capability for Paging" IE in S1 "UE-CAPABILITY-INFO-INDICATION" message from eNB. Otherwise, this field displays N/A.
Supported Codec List	The Supported Codec List information received by an MME service for connected UE in UE capability exchange message.
Mobile Station Classmark 2	The Mobile Station Classmark 2 information received by an MME service for connected UE in UE capability exchange message.
Mobile Station Classmark 3	The Mobile Station Classmark 3 information received by an MME service for connected UE in UE capability exchange message.
Security Mode Information	This group shows the status of NAS integrity check and NAS ciphering along with applicable algorithm as security mode information. It contains following information: • NAS Integrity Check • NAS Integrity Check Algorithm • NAS Ciphering • NAS Ciphering Algorithm
Active ENodeB information	This group shows the information of active eNodeB serving to this session.
Global ENodeB ID	The global identifier of active eNodeB serving to this session.
S1AP End Point	The IP address used by eNodeB on S1AP interface to connect with MME service.
Crypto-map Name	The name of the crypto map supporting this EnodeB association.
MME UE S1AP ID	Indicates the session identifier between MME and UE on S1AP interface serving to this session.
ENodeB UE S1AP ID	Indicates the session identifier between eNodeB and UE on S1AP interface serving to this session.
MME UE S1AP ID (stack):	Indicates up to three MME UE S1AP session identifiers present in this S1AP stack.
ENodeB UE S1AP ID (stack):	Indicates up to three eNodeB UE S1AP session identifiers present in this S1AP stack.
Total S1AP ID (stack)	Indicates the total count of S1AP session identifiers present in the stack.
Idle Mode Information Data	This group shows the information for the sessions in ECM idle mode.
Last TAI	Tracking Area Identity of the last Tracking Area visited by UE.

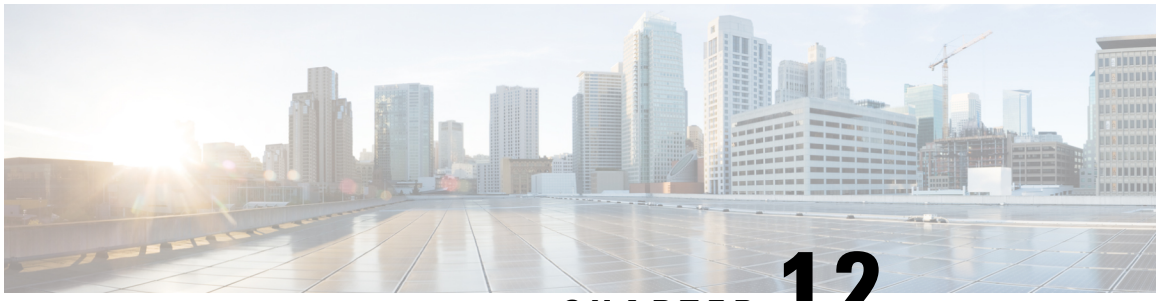
Field	Description
Last ECGI	E-UTRAN Cell Global Identifier of the last Cell visited by UE.
Last Connected ENodeB	Displays information about the ENodeB to which the session was last connected. • **Global ENodeB ID:** Global ENodeB Identifier of the ENodeB to which the UE last connected. • **S1AP End Point:** End Point IP Address of the ENodeB to which the UE last connected.
UE Subscription Data	This group shows the subscribed aggregate maximum bit rate applicable for connected UE in this session.
UE-UL-AMBR	The subscribed aggregate maximum bit rate in bits per second in upload traffic for connected UE in this session.
UE-DL-AMBR	The subscribed aggregate maximum bit rate in bits per second in download traffic for connected UE in this session.
Enforced UE-UL-AMBR at eNodeB	The enforced aggregate maximum bit rate in bits per second in upload traffic for connected UE at eNodeB in this session.
Enforced UE-DL-AMBR at eNodeB	The enforced aggregate maximum bit rate in bits per second in download traffic for connected UE at eNodeB in this session.
PDN Information	This group shows the information of PDNs connected for this session.
APN Name	The APN name which is serving for this PDN in this session.
UE Requested APN	Displays the UE requested APN with non-standard characters in hexadecimal format and standard characters in normal string format.
APN Restriction	The total number of APN restriction applied to this PDN.
PDN Type	The type of PDN (IPv4 and/or IPv6) which is serving in this session for PDN.
PGW Address	The IP address of the P-GW which is serving this session for connected PDN.
PGW control TEID	The control tunnel end identifier at P-GW on S5/S8 interface for control messaging serving to this session.
UE IPv4 Address	The IP address allocated to UE while connected to PDN in this session.
APN-UL-AMBR	The applicable aggregate maximum bit rate in bits per second in upload traffic for APN serving this PDN.
APN-DL-AMBR	The applicable aggregate maximum bit rate in bits per second in download traffic for APN serving this PDN.
Bearer Suspension State	The current suspension state of the bearer.
CSG Cell Change Notification	Displays CSG Information Reporting as specified by the PGW. If enabled, the MME sends notification when the UE enters or leaves a closed CSG cell.

Field	Description
CSG Subscribed Hybrid Cell Change Notification	Displays CSG Information Reporting as specified by the PGW. If enabled, the MME sends notification when the UE enters or leaves a hybrid cell as a subscribed member of the CSG in question.
CSG Unsubscribed Hybrid Cell Change Notification	Displays CSG Information Reporting as specified by the PGW. If enabled, the MME sends notification when the UE enters or leaves a hybrid cell with unsubscribed (non-member) status of the CSG in question
Marked for Deletion	Displays whether the PDN has marked for deletion flag set.
APN Restoration Priority	Displays the priority for reactivating impacted PDNs following a P-GW Restart Notification (PRN) where 1 is highest priority, 16 is lowest.
Low Access Priority Indication	Displays whether this PDN has LAPI indicator set as received in PDN connectivity requests.
Bearer Id	The identifier used for bearer between eNodeB and S-GW while connected to PDN in this session.
QCI	The quality class identifier applicable for this MME session.
AMBR	The applicable aggregate maximum bit rate in bits per second in download/upload direction for APN serving this PDN.
S1U ENodeB TEID	Indicates the tunnel end identifier at eNodeB on S1-U interface serving to this session.
S1U SGW TEID	Indicates the tunnel end identifier at S-GW on S1-U interface serving to this session.
S5S8 PGW TEID	Indicates the tunnel end identifier at P-GW on S5/S8 interface serving to this session.
S1U ENodeB IPv4 Addr	Indicates the IPv4 address used at eNodeB while connecting to S-GW on S1-U interface serving to this session.
S1U ENodeB IPv6 Addr	Indicates the IPv6 address used at eNodeB while connecting to S-GW on S1-U interface serving to this session.
S1U SGW IPv4 Addr	Indicates the IPv4 address used at S-GW while connecting to eNodeB on S1-U interface serving to this session.
S1U SGW IPv6 Addr	Indicates the IPv6 address used at S-GW while connecting to eNodeB on S1-U interface serving to this session.
S5S8 PGW Addr	Indicates the IP address used at P-GW while connecting to S-GW on S5/S8 interface serving to this session.
ESM State	The EPS session Management status serving to this session.
Bearer Type	The type of bearer used for this session. Possible values are: • Default • Dedicated
ARP	The Allocation Retention Priority value assigned to the bearer. The HSS assigns the value for default bearers and the P-GW assigns it for dedicated bearers.

Field	Description
PCI	Specifies the ARP Pre-emption Capability Indicator, either Enabled or Disabled.
PVI	Specifies the ARP Pre-emption Vulnerability Indicator, either Enabled or Disabled.
PGW-C+SMF Selected	Specifies that Combined PGW-C/SMF selection indicator, either Yes or No.
Marked for Deletion	Displays whether the bearer has marked for deletion flag set.
Total PDNs	The total number of PDNs connected through this session for a subscriber.
Total Bearers	The total number of bearers created for UE to use in this session.
Max APN Restrictions	The maximum number of APN restrictions applied to this PDN.
Tracking Area Information	This group displays the tracking area information available for this session.
TAI of last TAU	The tracking area identifier used in last Tracking Area Update (TAU) message received for TAU procedure in this session.
Current Tracking Area List	The tracking area list used for TAU procedure in this session.
CSG Information	This group displays Closed Subscriber Group information relating to this session.
CSG ID at Last Connection	Displays the CSG ID for this session. This is a unique identifier within the scope of PLMN which identifies a Closed Subscriber Group (CSG) in the PLMN.
CSG Cell Type	Displays the Closed Subscriber Group cell access mode (type) for this session, either Closed or Hybrid.
CSG Membership Status	Displays if the session is a member of the cell's CSG. Possible values are Member or Non-Member.
Operator Policy Association	The operator policy associated with this PDN.
CSFB Information	This group displays the Circuit-Switched Fall Back configuration associated with the session.
SGS Assoc State	The state of the SGs association with the VLR for the UE as determined by the MME. Possible states are: • SGs-NULL: Specifies that there is no SGs association with the VLR for the UE. In this state, no fields in this group will display information. • LA_UPDATE_REQUESTED: Specifies that the MME has requested an update location from the VLR before sending a response to the UE • SGs-ASSOCIATED: Specifies that the MME has stored an SGs association for the UE.
SGS Service	The name of the configured SGs service associated with the session.
VLR	The name of the VLR, as configured in the SGs service, associated with the session.
LAI	The Location Area Identifier to which the UE is mapped.

Field	Description
Pool Area	The name of the configured Location Area Code (LAC) pool area associated with the SGs service and the session.
P-TMSI	The Packet-Temporary Mobile Subscriber Identifier allocated by the MSC for the UE.
Flags	The current active variables associated with the UE. Possible states are: • SMS-Only: Specifies that the UE is combined attached for SMS services only. • MME Reset Indicator: Specifies that the MME has restarted after a failure. • VLR Reliable Indicator: Specifies that the MME has received a reset indication from the VLR. • VLR Offload: Specifies that the UE is set to offload state. • Non-EPS Alert: Specifies that the VLR is requesting from the MME an indication when any signaling activity from the UE is detected.
CIoT Optimisation Information	Displays the CIoT optimization information.
NB-IoT RAT	Displays if the RAT type NB-IoT is either enabled or disabled.
Attach Without PDN Support	Displays if attach without PDN support is either enabled or disabled.
UE capable of operating in CE-mode-B	Displays "TRUE" or "FALSE" to indicate if UE is operating in CE Mode-B.
Access Profile Association	Displays the configured access-profile name.
DECOR Information:	
UE Usage type	Displays the configured UE usage types.
DCN Id	Displays the configured DCN identifier.
UE DC-NR Information:	
DC-NR capable UE	Indicates whether the UE is DCNR capable.
DC-NR operation allowed	Indicates whether the DCNR operation is allowed by MME for the DCNR capable UE.
UE N1-Mode Information	
N1-mode capable UE	Indicates whether the UE N1 mode information is allowed by MME for the N1-mode capable UE.

show mme-service session full all | grep Paging



CHAPTER 12

ePDG Interworking with SMF+P-GW-IWK Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	ePDG
Applicable Platform(s)	• ASR 5500-DPC2 • VPC-DI
Feature Default	Disabled - License Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *ePDG Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release

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

Feature Description

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

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

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

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

License Requirements

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

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

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

Standards Compliance

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

3GPP References

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

How it Works

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

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

Call Flow

Figure 1: ePDG Setup Procedure Call Flow

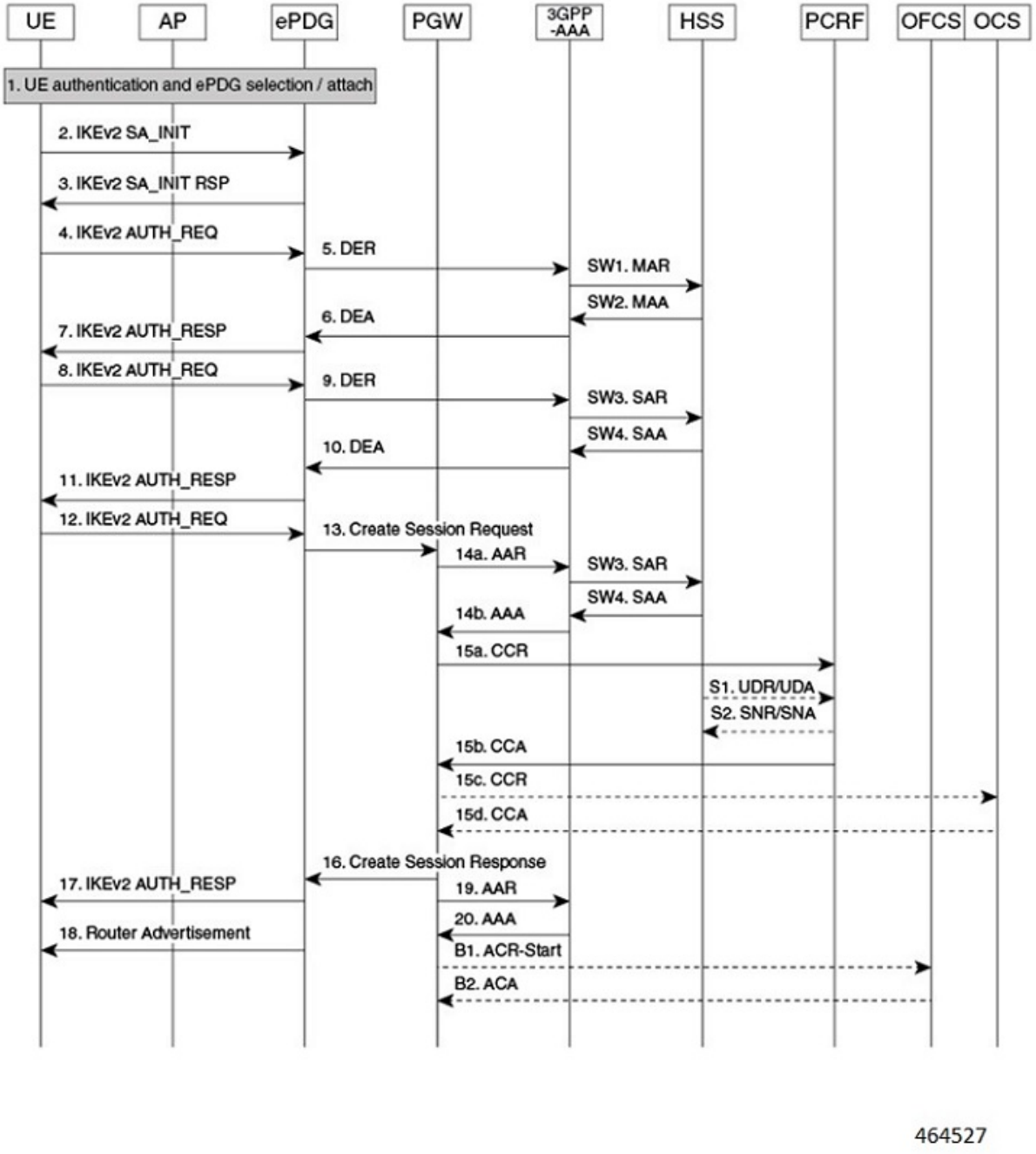


Table 5: ePDG Setup Procedure Call Flow Description

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

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

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

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

Information Element and AVP Support

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

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

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

Figure 2: P-GW or SMF+PGW-IWK Decision Matrix Table

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

464608

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

NOTE 1:

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

NOTE 2:

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

NOTE 3:

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

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

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

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

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

Fallback Mechanism for Selecting Combined SMF+PGW-IWK

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

Table 6: Fallback Mechanism

SMF+PGW-IWK or P-GW	Service Parameter	Selection Order
SMF+PGW-IWK	**x-s2b-gtp+nc-smf**	

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

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

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

Limitations

This feature has the following limitations:

- The ePDG support is applicable only for the 4G or 5G NAS capable devices attached to ePDG through the legacy 4G message. ePDG does not support 5G NAS request directly sent to ePDG.
- SMF+PGW-IWK support is limited to the GTPv2 based S2b interface.
- The emergency attach flow is not supported because for 5G NAS capable devices, the emergency VoWIFI call is not supported through ePDG.

Configuring ePDG to Enable 5G Interworking

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

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

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

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

NOTES:

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

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

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

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

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

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

```
configure
    context context_name
```

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

NOTES:

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

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

Configuring ePDG to Consider Interworking-5GS-Indicator

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

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

NOTES:

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

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

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

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

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

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

NOTES:

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

- **no**: Disables pgw-selection related parameters for the ePDG service.

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

Configuring ePDG in the Local SMF+PGW-IWK Node

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

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

NOTES:

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

Configuring ePDG 5G Interworking Bulk Statistics

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

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

NOTES:

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

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show epdg-service statistics interworking-5g

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

Table 7: show epdg-service statistics interworking-5g Command Output Descriptions

Field	Description
5G Sessions – Counter for sessions from N1 mode capable UEs	
Attempts	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE.
Setup	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE and that call succeeds.
Failures	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE and that call fails due to some failure reason.
P-GW/SMF selection type – Based on the 5G capability flags and related CLI, the PDN request is forwarded to P-GW or SMF+PGW-IWK	
SMF preferred	The number of times that SMF is chosen for this call, but IWK flag is not set.
SMF only	The number of times that ePDG selects SMF for this call, IWK flag is set, and PDU Session ID is forwarded to SMF.
DNS provided SMF	The number of times that SMF is selected from DNS responses.
Locally configured SMF	The number of times that SMF is selected from the local ePDG configuration.
AAA provided SMF IP	The number of times that ePDG selects SMF from the AAA server provided IP attribute.
P-GW only	The number of times P-GW is selected.
DNS provided P-GW	The number of times that P-GW is selected from DNS responses.
Locally configured P-GW	The number of times that P-GW is selected from the local ePDG configuration.
AAA provided P-GW IP	The number of times that P-GW is selected from the AAA server provided IP attribute.
P-GW or SMF not available reasons - Provide counters on how many times the SMF or P-GW selection is failed due to P-GW or SMF is not locally configured.	
No P-GW configured locally	The number of times that P-GW selection failed due to missing configuration.
No SMF configured locally	The number of times that SMF+PGW-IWK selection failed due to missing configuration.
SMF Fallback Support Statistics for GTP nodes – Fallback-related counters for SMF provided by AAA, DNS, and local configuration. In general, an attempt for second SMF or P-GW after the first SMF or P-GW is failed is considered as fallback.	
SMF Fallback Attempted	The number of times that fallback is attempted when SMF is preferred. Increments after it fails to connect to the first SMF and attempts the second SMF. This includes SMFs provided by AAA, DNS, and the local configuration.

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

Field	Description
P-GW Fallback Failure	The number of times that a session fails to connect to P-GW and selected through the fallback algorithm.
Alternate P-GW not found	The number of failed attempts to all P-GW, and there is no alternate P-GW available to attempt for a session to connect.
DNS-related Failures	
DNS server not reachable	The number of times when no response from DNS.
No resource records	The number of times that the DNS server responded with no resource records.
No matching P-GW service params	The number of times that the DNS server responded with no P-GW in the resource records, when P-GW is the preferred gateway for the session.
No matching SMF service params	The number of times that the DNS server responded with no SMFs in the resource records, when SMF is the preferred gateway for the session.
DNS P-GW list exhausted	The number of failed attempts to connect to all the P-GW provided by DNS response, when P-GW is the preferred gateway for the session.
DNS SMF list exhausted	The number of failed attempts to connect to all the SMF provided by DNS response, when SMF is the preferred gateway for the session.

show configuration

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

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

The following is a sample output:

```
config
  cli hidden
  tech-support test-commands encrypted password ***
    logging disable eventid 36012
  license key "\
  :
  :

epdg-service epdg1
  .....
  dns-pgw selection topology weight
  associate qci-qos-mapping epdg_mapping
```

```
 associate subscriber-map map1
 pgw-selection agent-info error-terminate
 pgw-selection ue-usage-type
 pgw-selection select pgw 4gonly-ue
 pgw-selection select pgw no-5gs-interworking
 associate lte-emergency-profile  emergency
 username check-mac-address failure-handling       continue
 reporting-action event-record
 max-sessions 100000
 bind address 111.111.11.2 crypto-template boston
#exit
```

show epdg-service name

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

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

The following is a sample output:

```
Service name:  epdg1
  Context: pdif
  Bind: Done
  Max Sessions : 100000
  MAG service : n/a
  MAG context : n/a
  PLMN Id:    MCC:242 , MNC:002
  Setup Timeout (sec) : 60
  dns-pgw context: pdif
  dns-pgw selection : weight,topology
  fqdn: n/a
  pgw-selection agent-info error-handling: terminate
  pgw-selection based on UE-Usage-Type: Enabled
  Custom SWm-SWu Error Mapping: Disabled
  Custom S2b-SWu Error Mapping: Disabled
  3GPP SWu Private Notify Error Types: Disabled
  Preferred PGW selection mechanism: AAA/DNS
  vendor-specific-attr dns-server-req: APCO
  PDN-type IPv6 Path-MTU   : Enabled
  GTPC Overload Control Profile :     None
  GTPC Load Control Profile:          None
  LTE Emergency Profile    : emergency
  Timeout Idle             : Disabled
  Associated PLMN list     : plmn1
  IR Handover Suppression  : Enabled
```

Bulk Statistics

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

show bulkstats variables epdg-interworking-5g

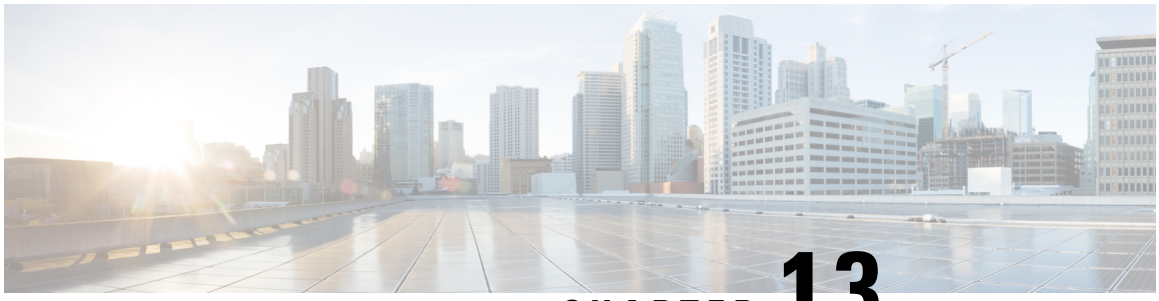
Use this command to display the list of bulk statistics variables supported by **epdg-interworking-5g schema**.

Bulk Statistics Variables	Description
5G Sessions:	
iwk5g-5gsessions-attempted	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE.
iwk5g-5gsessions-setup	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE and that call succeeds.
iwk5g-5gsessions-failure	The number of times that ePDG receives a call with N1_mode_capable (PDUSession) from UE and that call fails due to some failure reason.
P-GW/SMF selection type:	
iwk5g-smf-preferred	The number of times that SMF is selected as the first preference. Increments when SMF is chosen for this call, but the IWK flag is not set.
iwk5g-smf-preferred-dns	The number of times that SMF is selected from DNS responses.
iwk5g-smf-preferred-local	The number of times that SMF is selected in the local ePDG configuration.
iwk5g-smf-preferred-aaa	The number of times that ePDG selects the SMF in the AAA server provided IP attribute.
iwk5g-smf-only	The number of times when ePDG selects SMF for this call, IWK flag is set, and PDU Session ID is forwarded to SMF.
iwk5g-smf-only-dns	The number of times that SMF is selected from DNS responses.
iwk5g-smf-only-local	The number of times that SMF is selected in the local ePDG configuration.
iwk5g-smf-only-aaa	The number of times that ePDG selects the SMF from the AAA server provided IP attribute.
iwk5g-pgw-only	The number of times that P-GW is selected.

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

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

iwk5g-dns-smf-list-exhausted	The number of times that SMF provided by DNS response failed to connect, when SMF is the preferred gateway for the session.



CHAPTER 13

Handling CC-Request-Number AVP during Assume Positive State

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	Not Applicable

Revision History

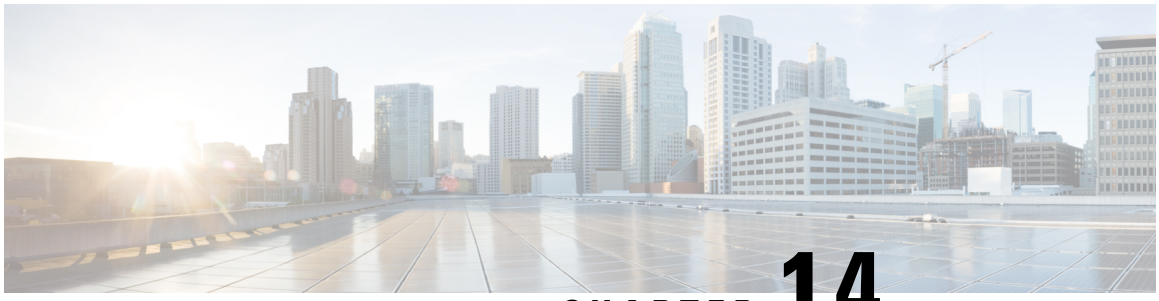
Revision Details	Release
P-GW supports handling of CC-Request-Number AVP during Assume Positive state.	21.26.h5
First Introduced.	21.26.19

Feature Changes

Previous behavior: In P-GW, the CC-Request-Number was incremented in the CCR-T message during the Assume Positive state.

New Behavior: The CC-Request-Number retains the same value as in the previous CCR-U message even for the CCR-T message during the Assume positive state.

Impact on Customer: The Online Charging System (OCS) can now read the proper CC-Request-Number for CCR-T message during the Assume positive state.



CHAPTER 14

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

Feature Summary and Revision History

Summary Data

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

Revision History

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

Feature Changes

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

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

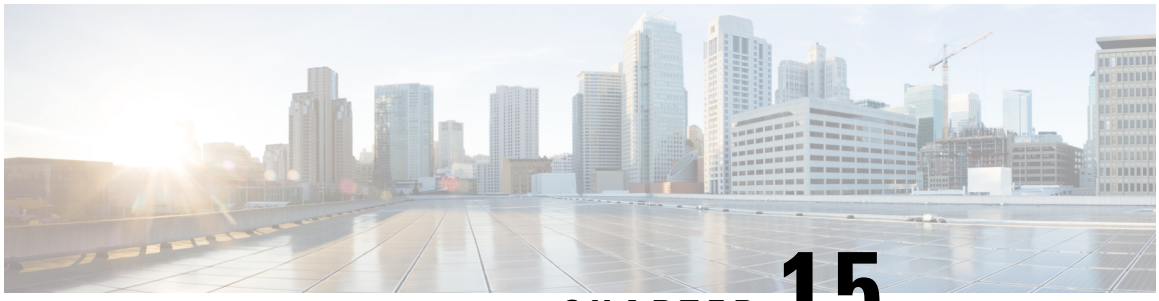
Command Changes

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

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

NOTES:

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



CHAPTER 15

IPv4 and IPv6 Address Alignment

Feature Summary and Revision History

Summary Data

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

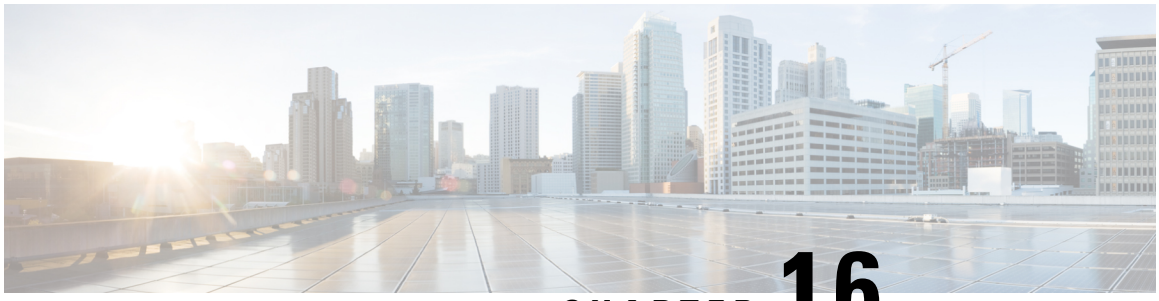
Revision History

Revision Details	Release
IPv4 and IPv6 address alignment is supported.	21.26

Feature Description

The User Equipment (UE) must consistently receive IP address assignment during Wi-Fi to LTE handover or conversely. For dual stack UEs requesting both addresses, due to the operator's choice and network preferences, UE receives either IPv4 or IPv6. In subsequent handovers, the UE will request based on the previously assigned IP address type. To ensure the IP address alignment between LTE to Wi-Fi HO or conversely, ePDG sends IPV4_ONLY_NOTIFICATION or IPV6_ONLY_NOTIFICATION in the IKE CFG_REPLY payload based on the allocated IP address. This feature complies with *3GPP TS 24.302 Release 15*.

For more information, see the *IPv4 and IPv6 Notification for IP Address Alignment* section in the *ePDG Administration Guide*.



CHAPTER 16

Monitoring Offloading and Onloading VPP Flow Transactions

Feature Summary and Revision History

Summary Data

Applicable Products or Functional Area	P-GW
Applicable Platforms	• 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* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

The P-GW is enhanced to collect log messages to monitor offloading and onloading flow transactions between the VPP and session manager. The logs are collected when traffic state changes from offloading to onloading, and conversely. The logs are stored in a file. Monitoring can be enabled or disabled using the supported CLI.

For more information, see the *VPP Metric Enhancement* chapter in the *P-GW Administration Guide*.

How it Works

P-GW supports a user-controlled mechanism to monitor traffic offloading to VPP, onloading to sessmgr, and collects the traffic statistics for the monitored period. When the feature is enabled, the logs are saved to */tmp/fpflowchangelog_2021-11-24_02h35m44sEST_1.csv*. Once the logging is disabled, the log file moves to */hd-raid/fpflowchangelog/fpflowchangelog_2021-12-16_04h06m55sEST_1.csv*. If the number of logs exceed 32K, the log file closes and moves to */hd-raid/fpflowchangelog/fpflowchangelog_2021-12-16_04h06m55sEST_2.csv*. Then, the new file gets created in the rotated index format. The number, for example, *_2.csv* gets incremented and gets saved to */tmp/fpflowchangelog_2021-11-24_02h35m44sEST* with the current stamp. However, the logging continues to happen as usual and the logs are written to the new file.

Enabling or Disabling Logging

The logs are stored in a file in the following format:

```
Timestamp,IMSI, Session-ID, Stream-Idx, Client-IP, Client-Port, Server-IP, Server-Port,
Protocol, Trigger-Type, Trigger-Reason
```

Use the following CLI command in the Exec mode to enable or disable offload and onload logging. By default, the monitoring is disabled:

logging session fp-flow-state-change facility sessmgr instance *instance_number* **number-of-events** *events_value*

logging session fp-flow-state-change facility sessmgr instance *instance_number* **duration** *duration_value*

You will receive the following warning message on enabling the command:

Warning Logging facility for flow state change is now enabled! Logs shall be written to /hd-raid/fpflowchangelog/fpflowchangelog_2021-12-16_04h06m55sEST_1.csv. Warning: Flow state change logging may have performance impact. Please use with discretion.

If the logging is already enabled when executing the command, you will receive the following message:

```
[local]laas-setup# logging session fp-flow-state-change facility sessmgr instance 8 duration
 10
Flow state change event logging is already enabled. Disable before enabling.
```

```
[local]laas-setup# logging session fp-flow-state-change facility sessmgr instance 12 duration
 10
Error in flow stream state change logging enable. Invalid parameter.
```

Note Once the configured value for **number-of-events** is met or the duration in seconds elapse, this feature gets disabled automatically.

The event logging must be enabled independent of any other feature or module log.

Monitoring and Troubleshooting

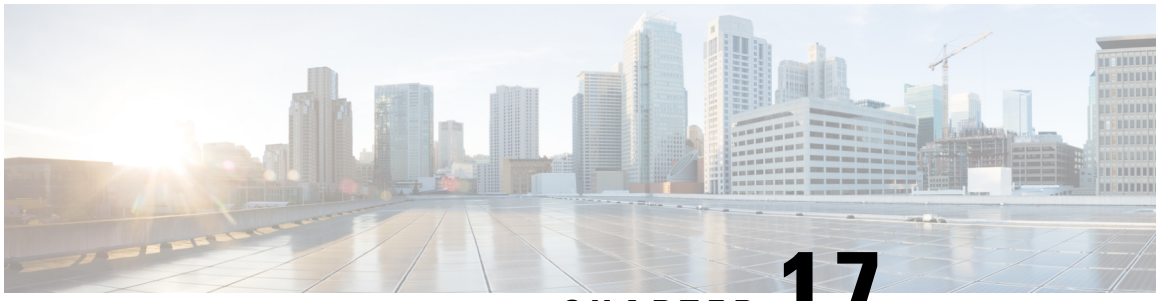
This section provides information to monitor and troubleshoot this feature using show commands.

Show Commands and Outputs

This section provides information about the show commands and outputs of offload and onload events.

show session fp-flow-state-change statistics

Field	Description
Onload/Offload event logging	Displays the status of logging to show if it is currently enabled or disabled.
Start time	Displays the start time of the last logging. If the logging was never started, the start time shows "NA".
End time	Displays the time when logging was stopped. If logging was never started, the end time shows NA. If the logging is currently enabled, it shows "In progress".
Total events recorded	Displays the total number of logs generated.
Logging enabled for *number of events/ duration*	The number of events or duration in seconds.
Sessmgr Instance	The session manager instance for which the logging is enabled.



CHAPTER 17

Multiple Customized PCO Support

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• GGSN • P-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* • *GGSN Administration Guide* • *P-GW Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
Support is added for additional Protocol Configuration Options, Custom6 through Custom10.	21.26

Revision Details	Release
Support is added to display a confirmation message before deleting or modifying an existing Container ID value in the Global Configuration mode.	21.24
Enhanced Protocol Configutaion Options (ePCO) support is added with the existing new operator defined PCO for UWB Indicator.	21.20.22
First introduced.	21.20.16

Feature Description

With the multiple PCO support feature, P-GW and GGSN sends customized Protocol Container Options (PCOs) to MS GTP messages. Custom1 is an existing PCO and its Container ID value is FF00H.

P-GW and GGSN support PCOs ranging from Custom1 through Custom10.

The global PCO container IDs are modified during runtime. This modification affects only the new subscriber sessions and doesn't affect the existing subscriber sessions. The PCO container IDs ranging from FF03 to FFFF are configurable.

Operator Defined PCO for Ultra Wideband (UWB) Indicator

P-GW supports either Protocol Configuration Options (PCO) or Enhanced Protocol Configuration Options (ePCO) based on the EPCOSI indication bit received from an UE in Create Session Request and Modify Bearer Request.

If the EPCOSI bit is set, P-GW sends PCO containers in the ePCO IE. If the EPCOSI bit isn't set, then P-GW sends PCO containers in PCO IE.

Note 3G (UMTS) PCO notification to the UE is added to support the Gn or Gp mode. GGSN doesn't support ePCO IE.

How it Works

This section describes the updation of PCO values using the Gx and Gy interfaces. The term Gateway (GW) is interchangeably used in this chapter for P-GW and GGSN.

Updating PCO Value Using Gx Interface

This section describes the procedure to update PCO values using the Gx interface.

- The Policy and Charging Rules Function (PCRF) sends a request to activate the predefined rules.
- If the activation is successful and if the charging action is configured for PCO, then the retrieved value is sent to the UE.

- If the predefined rule creation is performed during session creation (CCA), then the retrieved PCO is sent to the UE in Create Session Response for P-GW and Create PDP Context Response for GGSN.
- If the predefined rule activation is sent in the middle of the session (CCA-U), then the retrieved PCO is sent to the UE with the next message.
- The PCRF sends a request to deactivate predefined rules.
- If the removal of predefined rules is successful and if PCO is configured for charging action, then the configured value in the APN is returned to UE with the next message.
- If multiple predefined rules are enabled, then the last charging action configured for PCO, in the order of rules sent, is considered as valid and Session Manager is updated with the value.

Note Ensure that the last predefined rule has the correct PCO value for this scenario. The remaining requested rules will follow the regular predefined rule activation procedure.

Updating PCO Value Using Gy Interface

This section describes the procedure to update PCO values using the Gy interface.

- The Online Charging System (OCS) sends a filter ID to enable the corresponding post-processing dynamic rule.
- If the rule activation is successful and if the associated charging action is configured for PCO, then the retrieved value is sent to the Session Manager through the Session Update Indication event.
- The GW sends the PCO value to UE.
- If the OCS sends multiple filter IDs, then the charging action associated with the last filter ID is used for PCO.
- The CRF sends a request to deactivate the predefined rules.
- On successful removal of the predefined rules, if charging action is configured for PCO, then a default PCO value under APN will be returned to UE with the next message.

Configuring PCO

This section describes the PCO configuration. CLI modifications are not permitted when calls are active for APN Configuration mode and Global Configuration mode, but modifications are permitted for active-charging service.

Configuring PCO in Charging Action Mode

Use the following sample configuration to configure multiple PCOs in the ACS Charging Action Configuration Mode.

```
configure
  active-charging service service_name
```

```
      charging-action action_name
         { pco-custom1 | pco-custom2 | pco-custom3 | pco-custom4 |
pco-custom5 | pco-custom6 | pco-custom7 | pco-custom8 | pco-custom9 |
pco-custom10 } custom_value
        end
```

NOTES:

- **pco-custom1 - pco-custom10** *custom_value*: Configures multiple operator-specific PCOs. custom_value must be an integer in the range of 0-255.

Configuring Custom1 PCO in APN Configuration Mode

Use the following sample configuration to configure Custom1 PCO in the APN Configuration mode.

```
configure
   context context_name
      apn apn_name
         [ no ] pco-option custom1 [ ue-requested ]
         end
```

NOTES:

- **pco-option custom1**: Configures operator defined PCO container custom1 mode. By default, its container ID value is fixed to 0.
- **ue-requested**: Configures to include Custom PCO Options in PCO IE, only when it requested by UE.
- **no**: Removes custom1 PCO configuration in the APN Configuration mode.

Configuring Multiple PCOs in APN Configuration Mode

Use the following sample configuration to configure multiple PCOs in the APN Configuration mode.

```
configure
   context context_name
      apn apn_name
         [ no ] pco-options { { custom1 | custom2 | custom3 | custom4 |
custom5 | custom6 | custom7 | custom8 | custom9 | custom10 } [ ue-requested
 value custom_value | value custom_value ] }
        end
```

NOTES:

- **custom1 - custom10**: Configures APN to include custom PCO options in PCO IE.
- **ue-requested**: Configures to include custom PCO Options in PCO IE, only when it is requested by UE.
- **value** *custom_value* : Configures the default container value of custom PCO. custom_value must be an integer in the range of 0-255.
- **no**: Removes PCO configuration in the APN Configuration mode.

Configuring PCO Container ID in Global Configuration Mode

Use the following sample configuration to configure multiple PCOs in the Global Configuration mode.

```
configure
  [ no ] pco-options { custom2 | custom3 | custom4 | custom5 | custom6 |
 custom7 | custom8 | custom9 | custom10 } container-id container_id_value
  end
```

NOTES:

- **pco-options { custom2 - custom10}**: Configures custom PCO options in PCO IE.
- **container-id** *container_id_value*: Configures the operator defined container ID and the value ranging from FF03 to FFFF.
- **no**: Removes PCO container ID configuration in the Global Configuration mode.

Note The custom1 container ID is not configurable in the Global Configuration mode as its container value is fixed to FF00H.

Note If you delete or modify an existing container ID value for an ongoing session, it affects only the new sessions and does not affect the ongoing or existing sessions.

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

show active-charging charging-action all

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

Table 8: show active-charging charging-action all Command Output Descriptions

Field	Description
PCO-Custom1-10 value	Indicates the action value for multiple operator-specific PCOs. The value can range from 1 to 10.

show active-charging sessions full all

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

Table 9: show active-charging sessions full all Command Output Descriptions

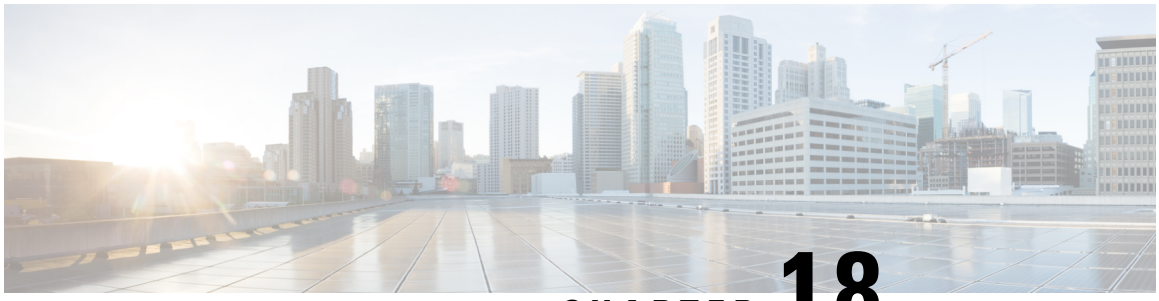
Field	Description
custom	Indicates Operator specific custom option.
Value	Indicates the value used for sending in custom PCO container.
Interface	Indicates the interface such as Gx. Gy or n/a based on the following conditions: • Gx: The charging rule is applied from the Gx interface that has custom PCO value. • Gy: The charging rule is applied from the Gy interface that has custom pco value. • n/a: The configured PCO value which is applied from APN profile.

show apn all

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

Table 10: show apn all Command Output Descriptions

Field	Description
Custom1-10 value	Specifies the action value for multiple operator-specific PCOs. The value can range from 1 to 10.
UE-Requested	Specifies PCO to the UE, which requested for new PCO option.



CHAPTER 18

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
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.	• 21.26 • 21.25.3
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.

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:

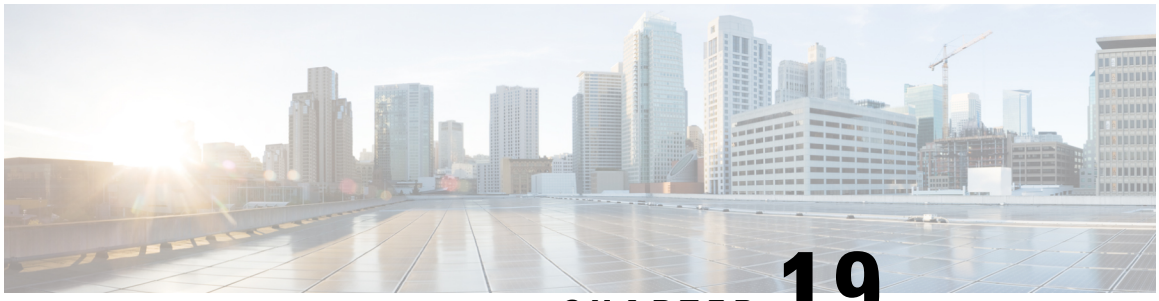
Use the **legacy-password-expiry** CLI command in the **save config** command, based on which new keywords are not saved. Configuration is stored in a format which previous release recognizes.

Use the following configuration under context configuration:

```
configure
   context host_name
     save configuration url [ confd | ignore-locks | 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 19

Password Change Option in Warning Period

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	StarOS
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Always-on
Related Changes in This Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Revision Details	Release
This feature supports a password change option in warning period.	• 21.26.h5 • 21.26.15

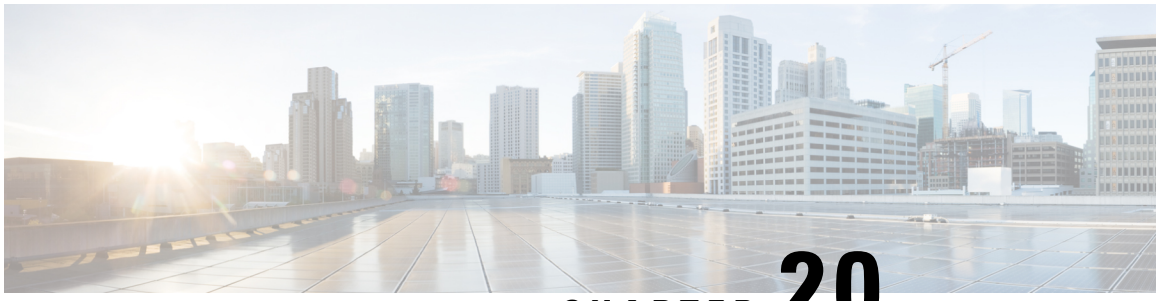
Feature Changes

Previous Behavior: When a warning about approaching password expiry is received, the change in password does not happen during the warning period when option "Y" is entered. The only way to change the password is with the configuration command.

New Behavior: You can change the password in the warning period.

```
When in warning period
1.Warning: Your password is about to expire in 3 days.
         We recommend you to change password.
         Logins are not allowed without acknowleding this.
         Do you want to change it now ? [y/n] (times out in 30 seconds) : n
# <you are logged in>
2.Warning: Your password is about to expire in 3 days.
         We recommend you to change password.
         Logins are not allowed without acknowleding this.
         Do you want to change it now ? [y/n] (times out in 30 seconds) : y
Auto generated password : <Jc42Q8hU>
Do you want to use auto-generated password? [y/n]: n
New password:
Repeat new password:
# <you are logged in>
```

Customer Impact: During Warning period user can change the password.



CHAPTER 20

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.	• 21.26 • 21.23.14
P-GW and S-GW supports secondary RAT usage reports and CDRs processing through GTPP Group Configuration CLIs.	21.20.31
First Introduced.	21.22.n7

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

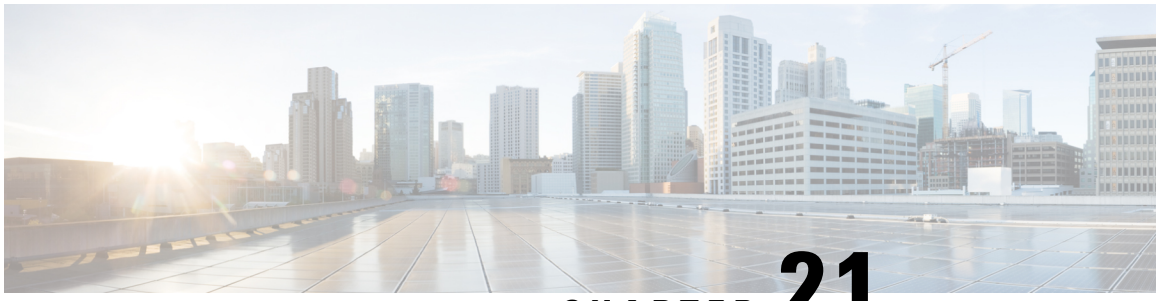
The output of this CLI command displays the following parameters.

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 21

Sponsored Data AVPs on Gx Interface to PCRF

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	• P-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	• *P-GW Administration Guide* • *SAEGW Administration Guide*

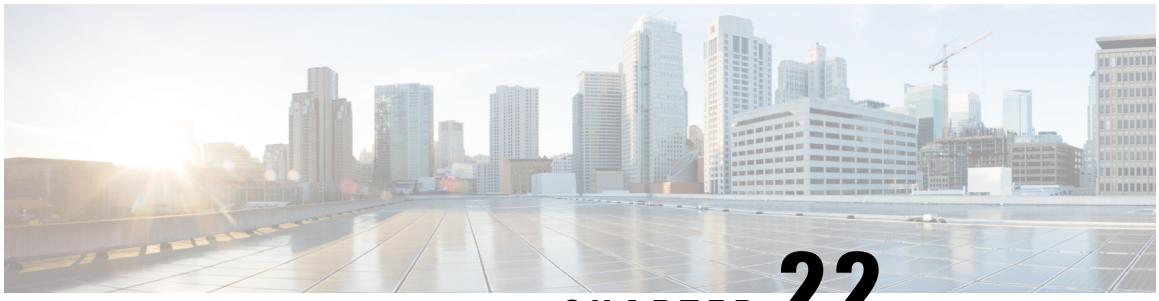
Revision History

Revision Details	Release
First introduced.	21.26

Feature Description

Sponsored connectivity is supported with the "dpca-custom8" Gx dictionary. When a session is enabled for sponsored connectivity from PCRF and offline charging is enabled using the aaa-custom4 dictionary, the sponsored connectivity AVPs are reported in the ACR Interim and ACR Stop packets to the CDF server. The Sponsor-Identity and Application-Service-Provider-Identity AVPs are sent under grouped AVP Service-Data-Container in ACR packets.

For more information, see the *Gx Interface Support* chapter in the *P-GW Administration Guide*.



CHAPTER 22

Support for 187 and 188 Information Element Types on S2b Interface

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	*P-GW Administration Guide*

Revision History

Revision Details	Release
Support for inclusion of 187 and 188 Information Element types on S2b Interface.	21.26.17

Feature Description

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

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

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

How it Works

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

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

Call Flow

Figure 3: Displays IEs Accross nodes

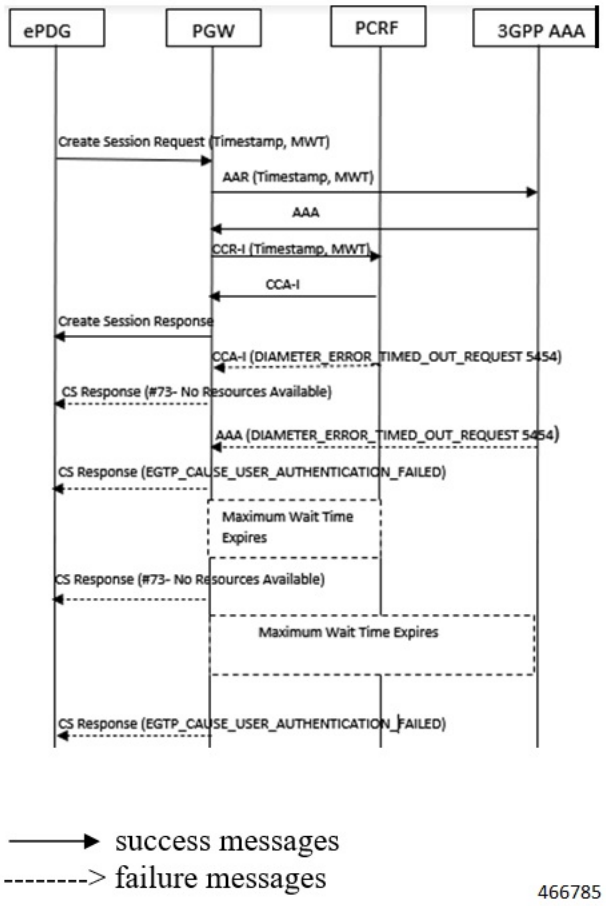


Table 11: Procedure

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

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

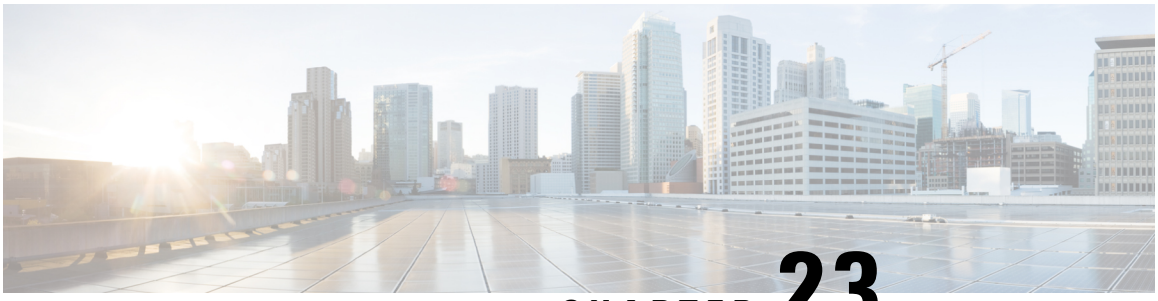
Supported RAT Types

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

Handling Handover

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

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



CHAPTER 23

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

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	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	*P-GW Administration Guide*

Revision History

Revision Details	Release
Support for inclusion of 187 and 188 Information Element types on S5 and S8 Interfaces.	21.26.17

Feature Description

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

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

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

GGSN on Gn/Gp interface is not supported.

How it Works

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

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

Call Flow

Figure 4: Displays IEs Accross nodes

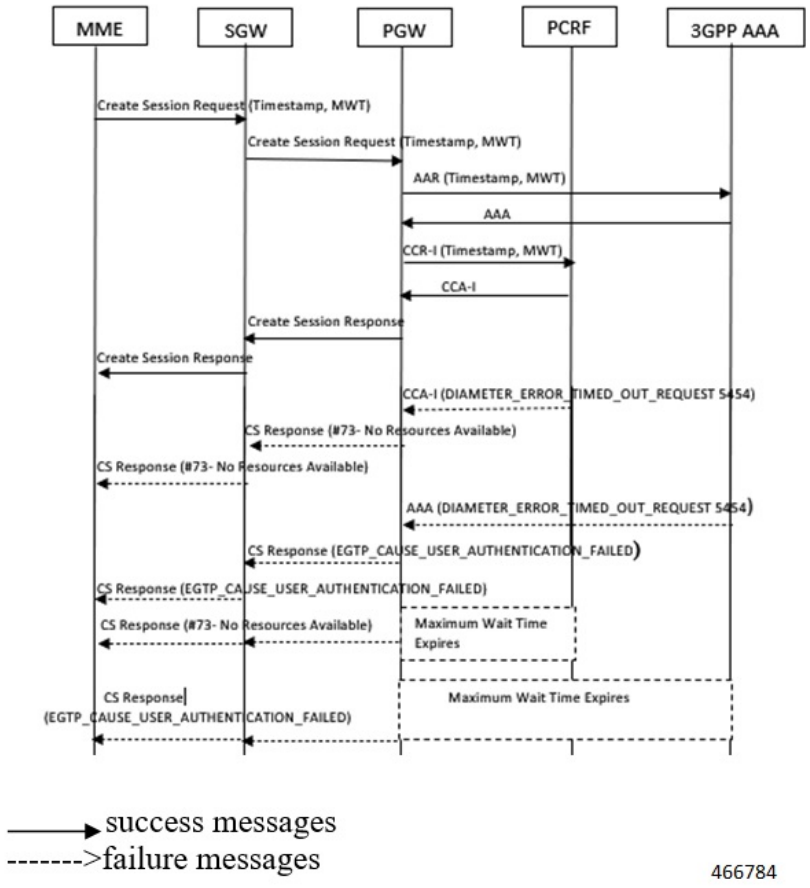


Table 12: Procedure

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

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

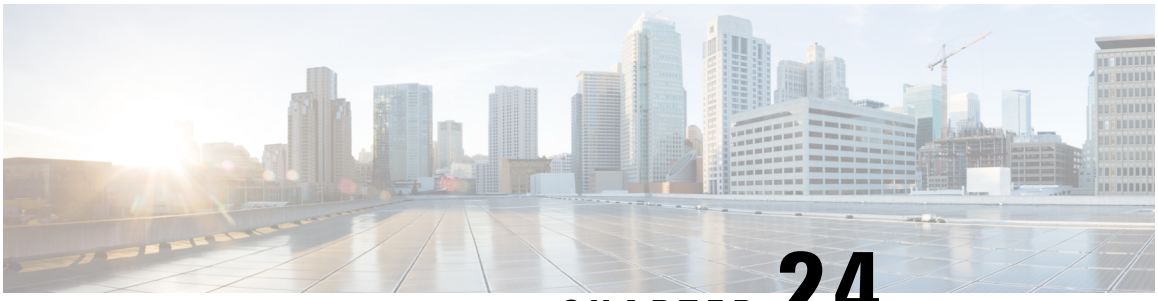
Supported RAT Types

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

Handling Handover

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

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



CHAPTER 24

VPP Flow Statistics

Feature Summary and Revision History

Summary Data

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

Revision History

Revision Details	Release
The **show active-charging flows full all** and **show active-charging flows summary** commands are enhanced to get the statistics from VPP.	21.26
The P-GW is enhanced to collect the log messages to monitor offloading and onloading flow transactions between VPP and the session manager.	21.26
The following enhancements were introduced: • Analyzer level statistics (TCP, UDP, P2P, HTTP, HTTPS) • VPP statistics collection using the CLI configuration	21.25
First introduced.	21.24

Feature Description

The **show active-charging flows full** command is enhanced to receive the per flow information from VPP. This command displays the VPP stream to flow mapping information.

The **show active-charging flows full** and **show active-charging flows summary** commands support the following filters:

- imsi
- ip-address
- msisdn
- username
- callerid
- flow-id
- session-id
- instance

For more information, see the *VPP Metric Enhancement* chapter in the *P-GW Administration Guide*.

Monitoring and Troubleshooting

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

Show Commands and Outputs

This section provides information about the show commands and outputs of VPP stream to flow mapping information for the CLI.

show active-charging flows full

Table 13: show active-charging flows full Command Output Descriptions

Field	Description
FP-Stream-ID (Up)	Specifies the fastpath stream ID of uplink packets.
FP-Stream-State (Up)	Specifies the fastpath stream state of uplink packets.
FP-Stream-ID (Down)	Specifies the fastpath stream ID of downlink packets.
FP-Stream-State (Down)	Specifies the fastpath stream state of downlink packets.
FP-Client-ID	Specifies the VPP fastpath client ID.
Offload-Stream-at-packet (up)	Specifies the packet number of a stream offloaded from the session manager to VPP when the uplink traffic starts.
Offload-Stream-at-packet (Down)	Specifies the packet number of a stream offloaded from the session manager to VPP when the downlink traffic starts.
VPP FP UL Packets	Specifies the VPP count for uplink packets.
VPP FP UL Bytes	Specifies the VPP count for uplink bytes.
VPP FP DL Packets	Specifies the VPP count for downlink packets.
VPP FP DL Bytes	Specifies the VPP count for downlink bytes.
VPP FP Packets	Specifies the total number of offloaded fastpath packets.
VPP FP Dropped Packets	Specifies the total number of dropped packets by VPP.
VPP Onload Succeeded	Specifies the total number of packets onloaded from VPP (onloaded to session manager).
Flow-ID	Identifier for flows.
Session-ID	Identifier for ACS session.
Uplink Packets	The total number of uplinked packets.
Uplink Bytes	The total number of uplinked bytes.
Downlink Packets	The total number of downlinked packets.
Downlink Bytes	The total number of downlinked bytes.
FP Packets	The number of data packets processed in fastpath for this flow.
MS IP	The MS IP address.

Field	Description
MS NAT IP	The MS NAT IP address.
Server IP	The server IP address.
Transport Protocol	The transport protocol: TCP, UDP, ICMP
Application Protocol	The application protocol.
Video Pacing	Indicates whether video pacing is enabled or disabled.
Video Encoded Bit Rate	The currently enforced bit rate for video pacing.
Video Pacing Initial Burst Size	The initial burst size allowed, in bytes, during video pacing.
Video Pacing Normal Burst Size	The normal burst size allowed, in bytes, during video pacing.
Video Pacing Dropped Bytes	The number of data bytes dropped during video pacing.
Video Payload Bytes Sent towards User	The number of data bytes sent to the UE during video pacing.
Video Pacing Duration	The total number of video pacing in seconds.
TCP MS Port	The TCP MS port number.
TCP MS NAT Port	The TCP MS NAT port number. This field is not displayed for one-to-one NAT.
TCP Server Port	The TCP server port number.
TCP State	Indicates the TCP state.
TCP Prev State	Indicates the previous TCP state.
MS Window Size	The mobile window size.
Server Window Size	The server window size.
MS Retries	The total number of mobile subscriber retries.
Server Retries	The total number of server retries.
ITC Action Applied	Indicates that the ITC action is applied.
Throttle-Suppress Countdown	Displays the configured timeout (elapsed time) when flow is throttle suppressed.
Throttle-Suppress	Displays "n/a" when throttle suppress is inactive.
Socket Migration Details:	TCP Proxy Socket Migration related information.
State	Indicates the Socket Migration state of the flow. For example, SOCK_MIG_DONE.
Highest ACK Frm Server	The highest acknowledgment number from the server.

Field	Description
Highest Seq Frm Server	The highest sequence number from the server.
Highest ACK Frm MS	The highest acknowledgement number from the MS.
Highest Seq Frm MS	The highest sequence number from the MS.
Seq Frm MS at Mig	The sequence number from MS at migration.
ACK Frm MS at Mig	The acknowledgement number from MS at migration.
Seq Frm Server at Mig	The sequence number from the server at migration.
ACK Frm Server at Mig	The acknowledgement number from the server at migration.
Data To Be Delivered To MS	Data to be delivered to the MS.
Data To Be Delivered To Server	Data to be delivered to the server.
Highest Seq Frm MS	The highest sequence number from the MS.
Timestamps Enabled	Indicates if timestamps option is enabled.
SACK Enabled	Indicates if selective acknowledgement is enabled.
Wscale From MS	The window scale value from MS.
Wscale From Server	The window scale value from the server.
Buffering Statistics:	
Buffered Uplink Packets	The total number of buffered uplink packets.
Buffered Uplink Bytes	The total number of buffered uplink bytes.
Buffered Downlink Packets	The total number of buffered downlink packets.
Buffered Downlink Bytes	The total number of buffered downlink bytes.
Uplink Packets in Buffer	The total number of uplink packets in the buffer.
Uplink Bytes in Buffer	The total number of uplink bytes in the buffer.
Downlink Packets in Buffer	The total number of downlink packets in the buffer.
Downlink Bytes in Buffer	The total number of downlink bytes in the buffer.
Buff Over-limit Uplink Pkts	The total number of uplink packets that are over the limit in the buffer.
Buff Over-limit Uplink Bytes	The total number of uplink bytes that are over the limit in the buffer.
Buff Over-limit Downlink Pkts	The total number of downlink packets that are over the limit in the buffer.
Buff Over-limit Downlink Bytes	The total number of downlink bytes that are over the limit in the buffer.
CAE-Readdressing:	

Field	Description
Requests CAE-Readdressed	The total number of request readdressing done.
Responses CAE-Readdressed	The total number of response readdressing done.
Requests having xheader inserted	The total number of HTTP requests with x-headers inserted.
Total connect failed to CAE	The total number of connections failed to the CAE.
Total CAE-Readdressed Uplink Bytes	The total number of uplink bytes readdressed.
Total CAE-Readdressed Uplink Packets	The total number of uplink packets readdressed.
Total CAE-Readdressed Downlink Bytes	The total number of downlink bytes readdressed.
Total CAE-Readdressed Downlink Packets	The total number of downlink packets readdressed.
Flows connected to CAE	The total number of flows connected to the CAE.
Proxy Disable Success	The total number of flows with proxy disabled.
Proxy Disable Failed	The total number of times the proxy disable function failed.
Link Monitoring	
Average Throughput	The average TCP throughput of downlink TCP traffic towards the mobile device, in kbps.
Average RTT	The average TCP RTT (Round Trip Time) of downlink TCP traffic towards the mobile device, in milliseconds.
Tethering detection performed	Indicates whether tethering detection was performed.
Tethering detected	Indicates whether tethering was detected.
Total ACS flows matching specified criteria	The total number of ACS flows that match the specified criteria.

show active-charging flows summary

Table 14: show active-charging flows summary Command Output Descriptions

Field	Description
Current:	
Active Flows	Specifies the total number of active flows currently on the system.
TCP Active flows	Specifies the total number of active flows for TCP traffic.
DNS Active flows	Specifies the total number of active flows for DNS traffic.
ICMPV6 Active flows	Specifies the total number of active flows for ICMPv6 traffic.
Idle Flows:	

Field	Description
TCP Idle flows	Specifies the total number of idle flows for TCP traffic.
UDP Idle flows	Specifies the total number of idle flows for UDP traffic.
ICMPv6 Idle flows	Specifies the total number of idle flows for ICMPv6 traffic.
DNS Idle flows	Specifies the total number of idle flows for DNS traffic.
Cumulative:	
Uplink Packets	Specifies the total number of uplinked packets.
Uplink Bytes	Specifies the total number of uplinked bytes.
Downlink Packets	Specifies the total number of downlinked packets.
Downlink Bytes	Specifies the total number of downlinked bytes.